

501P1376 US00

日 本 国 特 許 庁
JAPAN PATENT OFFICE



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2000年 9月 1日

出 願 番 号

Application Number:

特願2000-264923

出 願 人

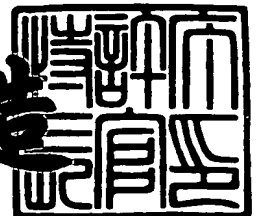
Applicant(s):

ソニー株式会社

2001年 6月28日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造



出証番号 出証特2001-3060859

【書類名】 特許願

【整理番号】 0000508204

【提出日】 平成12年 9月 1日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/00

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 山田 真

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 鶴飼 伸光

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 佐藤 順一

【発明者】

【住所又は居所】 東京都港区南青山 1 丁目 1 番 1 号 株式会社ソニーファイナンスインターナショナル内

【氏名】 川合 成幸

【発明者】

【住所又は居所】 東京都港区南青山 1 丁目 1 番 1 号 株式会社ソニーファイナンスインターナショナル内

【氏名】 奥出 勉

【発明者】

【住所又は居所】 東京都港区南青山 1 丁目 1 番 1 号 株式会社ソニーファイナンスインターナショナル内

【氏名】 伊藤 浩二

【特許出願人】

【識別番号】 000002185
【氏名又は名称】 ソニー株式会社
【代表者】 出井 伸之

【代理人】

【識別番号】 100082131
【弁理士】
【氏名又は名称】 稲本 義雄
【電話番号】 03-3369-6479

【手数料の表示】

【予納台帳番号】 032089
【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1
【包括委任状番号】 9708842

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理装置、および情報処理方法、電子マネーサービス提供システム、並びに記録媒体

【特許請求の範囲】

【請求項 1】 電子マネーサービスにおける電子マネーブランドの管理、並びに、前記電子マネーサービスの提携事業者の開拓および管理を行う第 1 の事業者が管理する情報処理装置において、

電子マネー情報、および前記電子マネーサービスに関する認証処理に用いられる認証情報が記録される第 1 の情報処理装置を発行する第 2 の事業者が管理する第 2 の情報処理装置と情報を授受する第 1 の授受手段と、

前記電子マネーを利用したサービスを提供する第 3 の事業者が管理する第 3 の情報処理装置と情報を授受する第 2 の授受手段と、

前記電子マネーサービスに関する認証処理に用いられる前記認証情報を記録する第 1 の記録手段と、

前記第 2 の事業者に関する情報、および前記第 1 の事業者と前記第 2 の事業者との提携内容に関する情報を記録する第 2 の記録手段と、

前記第 3 の事業者に関する情報、および前記第 1 の事業者と前記第 3 の事業者との提携内容に関する情報を記録する第 3 の記録手段と

を備え、

前記第 1 の授受手段は、前記第 2 の記録手段により記録された前記第 1 の事業者と前記第 2 の事業者との提携内容に関する情報に基づいて、前記第 1 の記録手段により記録された前記認証情報を出力し、

前記第 2 の授受手段は、前記第 3 の記録手段により記録された前記第 1 の事業者と前記第 3 の事業者との提携内容に関する情報に基づいて、前記第 1 の記録手段により記録された前記認証情報を出力する

ことを特徴とする情報処理装置。

【請求項 2】 前記認証情報は、DES を適応した秘密鍵情報を含むことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】 前記第 2 の事業者との課金処理を実行する第 1 の課金手段と、

前記第 3 の事業者との課金処理を実行する第 2 の課金手段と
を更に備えることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 4】 前記第 1 の記録手段により記録された前記認証情報を用いた認証処理を実行する認証手段を更に備え、

前記認証手段は、前記第 2 の授受手段により、前記第 3 の事業者より認証処理の実行を要求する信号が入力された場合、前記第 1 の記録手段により記録された前記第 3 の事業者に対応する前記認証情報を用いて認証処理を実行することを特徴とする請求項 1 に記載の情報処理装置。

【請求項 5】 前記第 1 の情報処理装置に記録された前記電子マネー情報を書き換える処理を行う第 4 の情報処理装置と、ネットワークを介して情報を授受する第 3 の授受手段と、

前記第 4 の情報処理装置に、前記第 1 の情報処理装置に対する前記電子マネーの充填処理を実行させるための制御信号を生成する生成手段と
を更に備え、

前記生成手段は、前記第 2 の記録手段により記録された、前記第 1 の事業者と前記第 2 の事業者との提携内容に関する情報に基づいて、前記第 2 の事業者が発行した前記第 1 の情報処理装置に対する前記制御信号を生成し、

前記第 3 の授受手段は、前記生成手段により生成された前記制御信号を、前記第 4 の情報処理装置へ出力する

ことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 6】 前記ネットワークは、インターネットであり、

前記第 3 の授受手段は、更に、前記インターネット上に仮想店舗を有する前記第 3 の事業者が管理する第 5 の情報処理装置と情報を授受する

ことを特徴とする請求項 7 に記載の情報処理装置。

【請求項 7】 電子マネーサービスにおける電子マネーブランドの管理、並びに、前記電子マネーサービスの提携事業者の開拓および管理を行う第 1 の事業者が管理する情報処理装置の情報処理方法において、

電子マネー情報、および前記電子マネーサービスに関する認証処理に用いられる認証情報が記録される第 1 の情報処理装置を発行する第 2 の事業者が管理する

第 2 の情報処理装置と情報を授受する第 1 の授受ステップと、

前記電子マネーを利用したサービスを提供する第 3 の事業者が管理する第 3 の情報処理装置と情報を授受する第 2 の授受ステップと、

前記電子マネーサービスに関する認証処理に用いられる前記認証情報を記録する第 1 の記録ステップと、

前記第 2 の事業者に関する情報、および前記第 1 の事業者と前記第 2 の事業者との提携内容に関する情報を記録する第 2 の記録ステップと、

前記第 3 の事業者に関する情報、および前記第 1 の事業者と前記第 3 の事業者との提携内容に関する情報を記録する第 3 の記録ステップと

を含み、

前記第 1 の授受ステップの処理では、前記第 2 の記録ステップの処理により記録された前記第 1 の事業者と前記第 2 の事業者との提携内容に関する情報に基づいて、前記第 1 の記録ステップの処理により記録された前記認証情報を出力し、

前記第 2 の授受ステップの処理では、前記第 3 の記録ステップの処理により記録された前記第 1 の事業者と前記第 3 の事業者との提携内容に関する情報に基づいて、前記第 1 の記録ステップの処理により記録された前記認証情報を出力することを特徴とする情報処理方法。

【請求項 8】 電子マネーサービスにおける電子マネーブランドの管理、並びに、前記電子マネーサービスの提携事業者の開拓および管理を行う第 1 の事業者が管理する情報処理装置用のプログラムであって、

電子マネー情報、および前記電子マネーサービスに関する認証処理に用いられる認証情報が記録される第 1 の情報処理装置を発行する第 2 の事業者が管理する第 2 の情報処理装置と情報を授受する第 1 の授受ステップと、

前記電子マネーを利用したサービスを提供する第 3 の事業者が管理する第 3 の情報処理装置と情報を授受する第 2 の授受ステップと、

前記電子マネーサービスに関する認証処理に用いられる前記認証情報を記録する第 1 の記録ステップと、

前記第 2 の事業者に関する情報、および前記第 1 の事業者と前記第 2 の事業者との提携内容に関する情報を記録する第 2 の記録ステップと、

前記第3の事業者に関する情報、および前記第1の事業者と前記第3の事業者との提携内容に関する情報を記録する第3の記録ステップと

を含み、

前記第1の授受ステップの処理では、前記第2の記録ステップの処理により記録された前記第1の事業者と前記第2の事業者との提携内容に関する情報に基づいて、前記第1の記録ステップの処理により記録された前記認証情報を出力し、

前記第2の授受ステップの処理では、前記第3の記録ステップの処理により記録された前記第1の事業者と前記第3の事業者との提携内容に関する情報に基づいて、前記第1の記録ステップの処理により記録された前記認証情報を出力する

ことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項9】 電子マネーサービスにおける電子マネーブランドの管理、並びに、前記電子マネーサービスの提携事業者の開拓および管理を行う第1の事業者が管理する第1の情報処理装置と、

電子マネー情報、および前記電子マネーサービスに関する認証処理に用いられる認証情報が記録される第2の情報処理装置と、

前記第2の情報処理装置を発行する第2の事業者が管理する第3の情報処理装置と、

前記電子マネーを利用したサービスを提供する第3の事業者が管理する第4の情報処理装置と

からなる電子マネーサービス提供システムにおいて、

前記第1の情報処理装置は、

前記第2の事業者が管理する第3の情報処理装置と情報を授受する第1の授受手段と、

前記第3の事業者が管理する第4の情報処理装置と情報を授受する第2の授受手段と、

前記電子マネーサービスに関する認証処理に用いられる前記認証情報を記録する第1の記録手段と、

前記第2の事業者に関する情報、および前記第1の事業者と前記第2の事業

者との提携内容に関する情報を記録する第 2 の記録手段と、
前記第 3 の事業者に関する情報、および前記第 1 の事業者と前記第 3 の事業者との提携内容に関する情報を記録する第 3 の記録手段と
を備え、
前記第 1 の授受手段は、前記第 2 の記録手段により記録された前記第 1 の事業者と前記第 2 の事業者との提携内容に関する情報に基づいて、前記第 1 の記録手段により記録された前記認証情報を出力し、
前記第 2 の授受手段は、前記第 3 の記録手段により記録された前記第 1 の事業者と前記第 3 の事業者との提携内容に関する情報に基づいて、前記第 1 の記録手段により記録された前記認証情報を出力し、
前記第 2 の情報処理装置は、
前記第 1 の授受手段によって、前記第 3 の情報処理装置へ出力された前記認証情報を記録する第 4 の記録手段と、
前記電子マネー情報を記録する第 5 の記録手段と
を備え、
前記第 3 の情報処理装置は、
前記第 1 の情報処理装置と情報を授受する第 3 の授受手段と、
前記第 3 の授受手段により入力された前記認証情報を記録する第 6 の記録手段と、
前記第 2 の情報処理装置の発行に関する情報を記録する第 7 の記録手段と、
前記第 6 の記録手段により記録された前記認証情報に基づいて、前記第 2 の情報処理装置との認証処理を実行する第 1 の認証処理実行手段と
を備え、
前記第 4 の情報処理装置は、
前記第 1 の情報処理装置と情報を授受する第 4 の授受手段と、
前記第 4 の授受手段により入力された前記認証情報を記録する第 8 の記録手段と、
前記第 8 の記録手段により記録された前記認証情報に基づいて、前記第 2 の情報処理装置との認証処理を実行する第 2 の認証処理実行手段と

を備える

ことを特徴とする電子マネーサービス提供システム。

【請求項 1 0】 前記第 3 の情報処理装置は、

前記第 2 の情報処理装置の前記第 5 の記録手段により記録された前記電子マネー情報を書き換える処理を実行する複数の第 5 の情報処理装置と情報を授受する第 5 の授受手段を更に備え、

前記第 1 の認証手段は、前記第 5 の授受手段により入力された、前記第 2 の情報処理装置の前記第 4 の記録手段により記録された前記認証情報に基づいて認証処理を実行する

ことを特徴とする請求項 9 に記載の電子マネーサービスシステム。

【請求項 1 1】 前記第 4 の情報処理装置は、

前記第 2 の情報処理装置の前記第 5 の記録手段により記録された前記電子マネー情報を書き換える処理を実行する複数の第 5 の情報処理装置と情報を授受する第 5 の授受手段を更に備え、

前記第 2 の認証手段は、前記第 5 の授受手段により入力された、前記第 2 の情報処理装置の前記第 4 の記録手段により記録された前記認証情報に基づいて認証処理を実行する

ことを特徴とする請求項 9 に記載の電子マネーサービスシステム。

【請求項 1 2】 前記第 4 の情報処理装置は、

前記第 2 の情報処理装置と情報を授受する第 5 の授受手段と、

前記第 2 の情報処理装置の前記第 5 の記録手段により記録された前記電子マネー情報を書き換えさせるための制御信号を生成する生成手段と

を更に備え、

前記第 2 の認証手段は、前記第 5 の授受手段により入力された、前記第 2 の情報処理装置の前記第 4 の記録手段により記録された前記認証情報に基づいて認証処理を実行する

ことを特徴とする請求項 9 に記載の電子マネーサービスシステム。

【請求項 1 3】 前記第 2 の情報処理装置は、

個人認証カード、入退出鍵、定期券、ポイントカード、会員カード、キャッシ

ユカード、クレジットカード、もしくはローンカードのうち、少なくとも一つの機能を実行するアプリケーションを記録する第9の記録手段を更に備える

ことを特徴とする請求項9に記載の電子マネーサービス提供システム。

【請求項14】 前記第2の情報処理装置は、非接触型ICカードであることを特徴とする請求項9に記載の電子マネーサービス提供システム。

【請求項15】 前記第2の情報処理装置は、接触型ICカードであることを特徴とする請求項9に記載の電子マネーサービス提供システム。

【請求項16】 前記第2の情報処理装置は、携帯電話機であることを特徴とする請求項9に記載の電子マネーサービス提供システム。

【請求項17】 前記第2の情報処理装置は、PDAであることを特徴とする請求項9に記載の電子マネーサービス提供システム。

【請求項18】 前記第2の情報処理装置は、パーソナルコンピュータであることを特徴とする請求項9に記載の電子マネーサービス提供システム。

【請求項19】 前記第2の情報処理装置は、時計であることを特徴とする請求項9に記載の電子マネーサービス提供システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報処理装置、および情報処理方法、電子マネーサービス提供システム、並びに記録媒体に関し、特に、電子マネー事業において、1つのブランドに対して、多くのイシューおよび加盟店が参画することができ、イシューおよび加盟店に対する暗号鍵の配布、およびシステムの運営・管理に必要なコストを低減することができる、情報処理装置、および情報処理方法、電子マネーサービス提供システム、並びに記録媒体に関する。

【0002】

【従来の技術】

電子マネーシステムや、セキュリティシステムにおいて、IC (Integrated circuit) カードの利用が増加している。ICカードとは、ICチップが埋め込まれたカード状デバイスのことであり、例えば、各種処理を行うCPU (Central

Processing Unit) などの演算処理部や、処理に必要なデータなどを記憶するメモリなどを内蔵している。ICカードは、所定のリーダ／ライタを利用して、電氣的に接触させた状態、もしくは、電磁波を利用した非接触の状態、データの読み書きが行われる。

【0003】

また、ICカードを、電子マネーシステムやセキュリティシステムなどで利用する場合においては、データの隠匿性や、ICカードの偽造を防止すること等のセキュリティが重要であり、データの記憶のためのリソース管理や、データに対するフレキシブルでセキュリティの高いアクセス制御を行うことが必要である。

【0004】

ICカードを用いた電子マネー事業は、電子マネーのブランドを管理するブランドホルダ、電子マネー事業における加盟店を開拓したり、管理するアクワイアラ、およびICカードを発行するイシュアの3つの機能により構築されている。

【0005】

従来、電子マネー事業は、ブランドホルダ、アクワイアラ、およびイシュアの3つの機能を一元的に行う事業体により行われているか、もしくは、それぞれのドメインを独立させ、1つのブランドホルダに対して、複数のアクワイアラおよび複数のイシュアが提携することにより行われてきた。

【0006】

【発明が解決しようとする課題】

しかしながら、ブランドホルダ、アクワイアラ、およびイシュアの3つの機能を一元的に有する1つの事業体により、電子マネー事業が行われる場合、その事業体は、電子マネー事業運営のためのシステム投資、加盟店用の端末装置などのハードウェアリソース、ICカードの発行および管理コストなどを全て負担した上で、事業運営を行わなければならない。電子マネーは、基本的にプリペイド（ユーザが先に入金、もしくは仮入金する）方式を採用していることから、他の決済方法（例えば、クレジットカードやデビットカードなど）より、手数料を高くすることはできないため、初期投資に対して、採算を上げることが困難であった。

【0007】

また、それぞれの事業ドメインを独立させ、1つのブランドホルダに対して、複数のアクワイアラおよび複数のイシューが提携することにより、電子マネー事業が行われる場合、事業運営のための初期投資を、各事業ドメインに分散して負担させることができるため、それぞれの1つの事業体としての初期投資の負担を軽減することができる。しかしながら、複数の事業体の提携による電子マネーシステムにおいては、その事業形態が複雑なものとなり、それぞれの事業ドメインに応じて、事業全体におけるレベニューシェアを行うことが困難である。

【0008】

そして、1枚のICカードが複数のサービス提供者によって相互運用される場合、あるサービス提供者が提供する固有のサービスに関する情報やアプリケーションは、相互運用する他のサービス提供者から許可なくアクセスできないようにしなければならない。そのようなセキュリティを維持しつつ、相互運用するサービスに関する情報やアプリケーションは、相互運用を実施しているサービス提供者で共有することができるようにしなければならない。

【0009】

しかしながら、ブランドホルダ、アクワイアラ、およびイシューをそれぞれ独立させた場合、事業ドメインの分散により、ICカードへの電子マネーの充填や、加盟店において電子マネーを利用するときに必要な認証処理に用いられる暗号鍵の配布および管理が複雑となるため、事業システムの維持・管理のコストアップにつながっていた。

【0010】

本発明はこのような状況に鑑みてなされたものであり、電子マネー事業において、1つのブランドに対して、多くのイシューおよび加盟店が参画することができ、イシューおよび加盟店に対する暗号鍵の配布、およびシステムの運営・管理に必要となるコストを低減することができるようにするものである。

【0011】

【課題を解決するための手段】

本発明の情報処理装置は、電子マネー情報、および電子マネーサービスに関す

る認証処理に用いられる認証情報が記録される第1の情報処理装置を発行する第2の事業者が管理する第2の情報処理装置と情報を授受する第1の授受手段と、電子マネーを利用したサービスを提供する第3の事業者が管理する第3の情報処理装置と情報を授受する第2の授受手段と、電子マネーサービスに関する認証処理に用いられる認証情報を記録する第1の記録手段と、第2の事業者に関する情報、および第1の事業者と第2の事業者との提携内容に関する情報を記録する第2の記録手段と、第3の事業者に関する情報、および第1の事業者と第3の事業者との提携内容に関する情報を記録する第3の記録手段とを備え、第1の授受手段は、第2の記録手段により記録された第1の事業者と第2の事業者との提携内容に関する情報に基づいて、第1の記録手段により記録された認証情報を出力し、第2の授受手段は、第3の記録手段により記録された第1の事業者と第3の事業者との提携内容に関する情報に基づいて、第1の記録手段により記録された認証情報を出力することを特徴とする。

【 0 0 1 2 】

認証情報は、DESを適応した秘密鍵情報を含むものとすることができる。

【 0 0 1 3 】

第2の事業者との課金処理を実行する第1の課金手段と、第3の事業者との課金処理を実行する第2の課金手段とを更に備えさせるようにすることができる。

【 0 0 1 4 】

第1の記録手段により記録された認証情報を用いた認証処理を実行する認証手段を更に備えさせるようにすることができ、認証手段には、第2の授受手段により、第3の事業者より認証処理の実行を要求する信号が入力された場合、第1の記録手段により記録された第3の事業者に対応する認証情報を用いて認証処理を実行させることができる。

【 0 0 1 5 】

第1の情報処理装置に記録された電子マネー情報を書き換える処理を行う第4の情報処理装置と、ネットワークを介して情報を授受する第3の授受手段と、第4の情報処理装置に、第1の情報処理装置に対する電子マネーの充填処理を実行させるための制御信号を生成する生成手段とを更に備えさせることができ、生成

手段には、第 2 の記録手段により記録された、第 1 の事業者と第 2 の事業者との提携内容に関する情報に基づいて、第 2 の事業者が発行した第 1 の情報処理装置に対する制御信号を生成させることができ、第 3 の授受手段には、生成手段により生成された制御信号を、第 4 の情報処理装置へ出力させることができる。

【 0 0 1 6 】

ネットワークは、インターネットであるものとすることができ、第 3 の授受手段には、更に、インターネット上に仮想店舗を有する第 3 の事業者が管理する第 5 の情報処理装置と情報を授受させることができる。

【 0 0 1 7 】

本発明の情報処理方法は、電子マネー情報、および電子マネーサービスに関する認証処理に用いられる認証情報が記録される第 1 の情報処理装置を発行する第 2 の事業者が管理する第 2 の情報処理装置と情報を授受する第 1 の授受ステップと、電子マネーを利用したサービスを提供する第 3 の事業者が管理する第 3 の情報処理装置と情報を授受する第 2 の授受ステップと、電子マネーサービスに関する認証処理に用いられる認証情報を記録する第 1 の記録ステップと、第 2 の事業者に関する情報、および第 1 の事業者と第 2 の事業者との提携内容に関する情報を記録する第 2 の記録ステップと、第 3 の事業者に関する情報、および第 1 の事業者と第 3 の事業者との提携内容に関する情報を記録する第 3 の記録ステップとを含み、第 1 の授受ステップの処理では、第 2 の記録ステップの処理により記録された第 1 の事業者と第 2 の事業者との提携内容に関する情報に基づいて、第 1 の記録ステップの処理により記録された認証情報を出力し、第 2 の授受ステップの処理では、第 3 の記録ステップの処理により記録された第 1 の事業者と第 3 の事業者との提携内容に関する情報に基づいて、第 1 の記録ステップの処理により記録された認証情報を出力することを特徴とする。

【 0 0 1 8 】

本発明の記録媒体に記録されているプログラムは、電子マネー情報、および電子マネーサービスに関する認証処理に用いられる認証情報が記録される第 1 の情報処理装置を発行する第 2 の事業者が管理する第 2 の情報処理装置と情報を授受する第 1 の授受ステップと、電子マネーを利用したサービスを提供する第 3 の事

業者が管理する第3の情報処理装置と情報を授受する第2の授受ステップと、電子マネーサービスに関する認証処理に用いられる認証情報を記録する第1の記録ステップと、第2の事業者に関する情報、および第1の事業者と第2の事業者との提携内容に関する情報を記録する第2の記録ステップと、第3の事業者に関する情報、および第1の事業者と第3の事業者との提携内容に関する情報を記録する第3の記録ステップとを含み、第1の授受ステップの処理では、第2の記録ステップの処理により記録された第1の事業者と第2の事業者との提携内容に関する情報に基づいて、第1の記録ステップの処理により記録された認証情報を出力し、第2の授受ステップの処理では、第3の記録ステップの処理により記録された第1の事業者と第3の事業者との提携内容に関する情報に基づいて、第1の記録ステップの処理により記録された認証情報を出力することを特徴とする。

【0019】

本発明の電子マネーサービス提供システムは、第1の情報処理装置が、第2の事業者が管理する第3の情報処理装置と情報を授受する第1の授受手段と、第3の事業者が管理する第4の情報処理装置と情報を授受する第2の授受手段と、電子マネーサービスに関する認証処理に用いられる認証情報を記録する第1の記録手段と、第2の事業者に関する情報、および第1の事業者と第2の事業者との提携内容に関する情報を記録する第2の記録手段と、第3の事業者に関する情報、および第1の事業者と第3の事業者との提携内容に関する情報を記録する第3の記録手段とを備え、第1の授受手段は、第2の記録手段により記録された第1の事業者と第2の事業者との提携内容に関する情報に基づいて、第1の記録手段により記録された認証情報を出力し、第2の授受手段は、第3の記録手段により記録された第1の事業者と第3の事業者との提携内容に関する情報に基づいて、第1の記録手段により記録された認証情報を出力し、第2の情報処理装置が、第1の授受手段によって、第3の情報処理装置へ出力された認証情報を記録する第4の記録手段と、電子マネー情報を記録する第5の記録手段とを備え、第3の情報処理装置が、第1の情報処理装置と情報を授受する第3の授受手段と、第3の授受手段により入力された認証情報を記録する第6の記録手段と、第2の情報処理装置の発行に関する情報を記録する第7の記録手段と、第6の記録手段により記

録された認証情報に基づいて、第2の情報処理装置との認証処理を実行する第1の認証処理実行手段とを備え、第4の情報処理装置が、第1の情報処理装置と情報を授受する第4の授受手段と、第4の授受手段により入力された認証情報を記録する第8の記録手段と、第8の記録手段により記録された認証情報に基づいて、第2の情報処理装置との認証処理を実行する第2の認証処理実行手段とを備えることを特徴とする。

【 0 0 2 0 】

第3の情報処理装置には、第2の情報処理装置の第5の記録手段により記録された電子マネー情報を書き換える処理を実行する複数の第5の情報処理装置と情報を授受する第5の授受手段を更に備えさせることができ、第1の認証手段には、第5の授受手段により入力された、第2の情報処理装置の第4の記録手段により記録された認証情報に基づいて認証処理を実行させることができる。

【 0 0 2 1 】

第4の情報処理装置には、第2の情報処理装置の第5の記録手段により記録された電子マネー情報を書き換える処理を実行する複数の第5の情報処理装置と情報を授受する第5の授受手段を更に備えさせることができ、第2の認証手段には、第5の授受手段により入力された、第2の情報処理装置の第4の記録手段により記録された認証情報に基づいて認証処理を実行させることができる。

【 0 0 2 2 】

第4の情報処理装置には、第2の情報処理装置と情報を授受する第5の授受手段と、第2の情報処理装置の第5の記録手段により記録された電子マネー情報を書き換えさせるための制御信号を生成する生成手段とを更に備えさせることができ、第2の認証手段には、第5の授受手段により入力された、第2の情報処理装置の第4の記録手段により記録された認証情報に基づいて認証処理を実行させることができる。

【 0 0 2 3 】

第2の情報処理装置には、個人認証カード、入退出鍵、定期券、ポイントカード、会員カード、キャッシュカード、クレジットカード、もしくはローンカードのうち、少なくとも一つの機能を実行するアプリケーションを記録する第9の記

録手段を更に備えさせることができる。

【 0 0 2 4 】

第 2 の情報処理装置は、非接触型 I C カードであるものとすることができる。

【 0 0 2 5 】

第 2 の情報処理装置は、接触型 I C カードであるものとすることができる。

【 0 0 2 6 】

第 2 の情報処理装置は、携帯電話機であるものとすることができる。

【 0 0 2 7 】

第 2 の情報処理装置は、 P D A であるものとすることができる。

【 0 0 2 8 】

第 2 の情報処理装置は、パーソナルコンピュータであるものとする
ことができる。

【 0 0 2 9 】

第 2 の情報処理装置は、時計であるものとすることができる。

【 0 0 3 0 】

本発明の情報処理装置、情報処理方法、および記録媒体に記録されているプログラムにおいては、電子マネー情報、および電子マネーサービスに関する認証処理に用いられる認証情報が記録される第 1 の情報処理装置を発行する第 2 の事業者が管理する第 2 の情報処理装置と情報が授受され、電子マネーを利用したサービスを提供する第 3 の事業者が管理する第 3 の情報処理装置と情報が授受され、電子マネーサービスに関する認証処理に用いられる認証情報が記録され、第 2 の事業者に関する情報、および第 1 の事業者と第 2 の事業者との提携内容に関する情報が記録され、第 3 の事業者に関する情報、および第 1 の事業者と第 3 の事業者との提携内容に関する情報が記録され、第 1 の事業者と第 2 の事業者との提携内容に関する情報に基づいて、認証情報が出力され、第 1 の事業者と第 3 の事業者との提携内容に関する情報に基づいて、認証情報が出力される。

【 0 0 3 1 】

本発明の電子マネーサービス提供システムにおいては、第 1 の情報処理装置で、第 2 の事業者が管理する第 3 の情報処理装置と情報が授受され、第 3 の事業者

が管理する第 4 の情報処理装置と情報が授受され、電子マネーサービスに関する認証処理に用いられる認証情報が記録され、第 2 の事業者に関する情報、および第 1 の事業者と第 2 の事業者との提携内容に関する情報が記録され、第 3 の事業者に関する情報、および第 1 の事業者と第 3 の事業者との提携内容に関する情報が記録され、第 1 の事業者と第 2 の事業者との提携内容に関する情報に基づいて、認証情報が出力され、第 1 の事業者と第 3 の事業者との提携内容に関する情報に基づいて、認証情報が出力され、第 2 の情報処理装置で、認証情報が記録され、電子マネー情報が記録され、第 3 の情報処理装置で、第 1 の情報処理装置と情報が授受され、入力された認証情報が記録され、第 2 の情報処理装置の発行に関する情報が記録され、記録された認証情報に基づいて、第 2 の情報処理装置との認証処理が実行され、第 4 の情報処理装置で、第 1 の情報処理装置と情報が授受され、入力された認証情報が記録され、記録された認証情報に基づいて、第 2 の情報処理装置との認証処理が実行される。

【 0 0 3 2 】

【発明の実施の形態】

以下、図を参照して、本発明の実施の形態について説明する。

【 0 0 3 3 】

図 1 は、本発明を適応した電子マネーシステムの構成を示す図である。運営本体としての、アクワイアラ・ブランドホルダ 1 は、自分自身のブランドの電子マネーに関するサービス（以下、本サービスと称する）の業務を運営するものであり、本サービスと提携しているイシュア 2 および店舗 4 に、自分自身が運営・管理するブランドの電子マネーに関する各種処理を実行するために必要となる、全ての「鍵」を管理し、必要に応じて、イシュア 2 もしくは店舗 4 に発行する。また、本サービスに参画する店舗 4 を開拓するのも、アクワイアラ・ブランドホルダ 1 の業務である。

【 0 0 3 4 】

アクワイアラ・ブランドホルダ 1 から発行される鍵は、秘密鍵であり、例えば、DES (Data Encryption Standard) などが用いられる。DES は、データを 64bit 単位に区切って暗号化および復号化処理を行う暗号システムである。DE

S アルゴリズムでは暗号化と復号化は対称であり、受信した暗号文を、同じ鍵を使ってもう一度変換することにより、元の情報を復元することができる。

【0035】

DES では、簡単なビット位置転置と XOR 演算の組み合わせ論理を 16 回繰り返している。内部的には、データのフィードバックや条件判断部分がなく、処理が逐次的なので、パイプライン化すれば高速に処理することができる。もともと LSI 化することを前提にして決められたアルゴリズムであり、DES チップも多く作られている。

【0036】

イシュア 2 は、例えば、銀行、クレジットカード会社、鉄道会社、その他の事業者である。アクワイアラ・ブランドホルダ 1 と提携したイシュア 2 は、その提携内容に従って、自社が発行する、例えば、IC カードなどに、アクワイアラ・ブランドホルダ 1 が管理・運営するブランドの電子マネーに関する機能を組み込み、アクワイアラ・ブランドホルダ 1 が発行する鍵を組み込むことができる。

【0037】

イシュア 2 が発行するハードウェアは、アクワイアラ・ブランドホルダ 1 が管理・運営するブランドの電子マネーに関する各種処理を実行するための機能を有し、鍵を安全に保持することができるものであれば、IC カードのみならず、例えば、携帯電話、PDA (Personal Digital (Data) Assistants)、パーソナルコンピュータ、もしくは、時計などの、様々な情報処理機器を用いることが可能である。ここでは、イシュア 2 が発行するハードウェアは IC カードであるものとして説明する。

【0038】

また、イシュア 2 により発行される IC カードは、電子マネーの利用以外の機能を有することが可能であり、例えば、社員証などの個人認証機能、建物や部屋などの入退出カード（電子キー）、定期券、ポイントカード、会員カード、キャッシュカード、クレジットカード、ローンカードなどの機能を有する（すなわち、IC カード内部に、それらの機能を実現するアプリケーションを記録させる）ことが可能である。

【0039】

利用者3、すなわちICカードの保有者は、イシュア2が発行したICカードに、イシュア2より発行された価値（すなわち、電子マネー）を記録させることができる。電子マネーに対応する代金は、現金、クレジットカード、もしくは、銀行口座の預金からの引き落としなどにより支払うことができる。利用者3は、ICカードに記録された電子マネーを用いて、本サービスに加盟している店舗4において、例えば、商品を購入したり、サービスの提供を受けるといった消費活動を行うことが可能である。

【0040】

店舗4は、アクワイアラ・ブランドホルダ1との提携によって、ICカードと各種情報を授受する場合の認証処理に必要な鍵の発行を受け、提携内容に基づいた各種サービスを利用者3に提供する。

【0041】

店舗4は、利用者3がICカードを利用して得た商品、もしくはサービスに対する代金を、アクワイアラ・ブランドホルダ1に請求する。アクワイアラ・ブランドホルダ1は、イシュア2に対して、代金の請求を行う。利用者3が保有するICカードに対する電子マネーの発行が、現金の入金と引き換えに行われた場合、イシュア2は、電子マネーの発行に対応する入金を既に得ているが、電子マネーの発行が、クレジットカード、もしくは、銀行口座の預金からの引き落としなどの支払方法によって行われた場合、イシュア2は、例えば、銀行やクレジット会社などの金融機関5に対して、電子マネーの発行に対応する代金の請求を行う。金融機関5は、クレジットカード、もしくは、銀行口座の預金からの引き落としなどの支払方法を利用した利用者3に対する従来の請求方法と同様の請求方法で、電子マネーの発行を受けた利用者3に、電子マネーに対応する料金を請求する。

【0042】

図2を用いて、アクワイアラ・ブランドホルダ1と、イシュア2、本サービスと提携した店舗4に設置されている各種端末装置、インターネット上に公開されている本サービスと提携したサイバー店舗、および、利用者3が有するパーソナ

ルコンピュータとのネットワーク接続の構成、および、アクワイアラ・ブランドホルダ 1 の鍵の発行について説明する。

【 0 0 4 3 】

アクワイアラ・ブランドホルダ 1 は、提携しているイシュー 2 - 1 および 2 - 2 に対して、その提携内容に従って、所定の鍵を発行する。イシュー 2 - 1 は、インターネット 1 1 を介して、利用者 3 へ、直接的なサービスの提供を行っていない。それに対して、イシュー 2 - 2 は、インターネット 1 1 を介して、利用者 3 へ、直接サービスの提供を行っている。イシュー 2 - 1 は、アクワイアラ・ブランドホルダ 1 が発行した鍵を内部に保持する IC カード 1 2 - 1 を利用者 3 に対して発行する。また、イシュー 2 - 1 は、IC カード 1 2 - 1 に電子マネーを充填するための入金端末装置 1 3 - 1 を管理する。同様に、イシュー 2 - 2 も、アクワイアラ・ブランドホルダ 1 が発行した鍵を内部に保持する IC カード 1 2 - 2 を利用者 3 に対して発行し、IC カード 1 2 - 2 に電子マネーを充填するための入金端末装置 1 3 - 2 を管理する。

【 0 0 4 4 】

ここでは、イシュー 2 - 1 およびイシュー 2 - 2 の 2 つのイシューがアクワイアラ・ブランドホルダ 1 と提携しているものとして説明しているが、インターネット 1 1 を介した利用者 3 へのサービスを行っていない複数のイシュー、およびインターネット 1 1 を介した利用者 3 へのサービスを行っている複数のイシューが、アクワイアラ・ブランドホルダ 1 と提携し、それぞれ、提携内容に基づいた鍵の発行を受け、その鍵を内部に保持した IC カードを利用者 3 に発行している。以下、イシュー 2 - 1 および 2 - 2 を個々に区別する必要がない場合、単にイシュー 2 と総称し、IC カード 1 2 - 1 および 1 2 - 2 を個々に区別する必要がない場合、単に IC カード 1 2 と総称し、入金端末装置 1 3 - 1 および 1 3 - 2 を個々に区別する必要がない場合、単に入金端末装置 1 3 と総称する。

【 0 0 4 5 】

アクワイアラ・ブランドホルダ 1 は、利用者 3 が、本サービスと提携している店舗 4 において、IC カード 1 2 を利用できるように（すなわち、IC カード 1 2 と、店舗 4 に備えられた端末装置との情報の授受が可能となるよう

に)、それぞれ、提携内容に基づいた鍵を発行する。アクワイアラ・ブランドホルダ1が行う、店舗4への鍵の発行方法は、大きく3つに分かれる。

【0046】

例えば、チェーン店などの複数の店舗4を有する企業が、本サービスと提携した場合、アクワイアラ・ブランドホルダ1は、それらの店舗を統括するPOS (Point of sale) センタ17に対して鍵を発行して配布する。POSセンタ17が管理する、それぞれの店舗4に設けられている加盟店端末装置18 (図2においては、加盟店端末装置18を1つだけ図示しているが、実際には、複数の店舗4に、それぞれ加盟店端末装置18が設置されている) は、POSセンタ17と、例えば、専用線を用いて接続されており、利用者3が、本サービスの電子マネーを、加盟店端末装置18において利用するとき、加盟店端末装置18は、POSセンタ17と接続することにより、ICカード12との認証処理を実行する。

【0047】

また、加盟店端末装置18が高度なタンパ技術 (半導体チップなどの内部解析や改ざんを物理的及び論理的に防衛する技術) を用いたものであれば、それぞれの加盟店端末装置18に、POSセンタ17に配布された鍵を記憶させて、加盟店端末装置18とICカード12間で認証処理を実行させるようにしても良い。

【0048】

なお、図2においては、POSセンタ17をひとつだけ図示して説明しているが、複数のPOSセンタ17が、その提携内容に基づいて、アクワイアラ・ブランドホルダ1から鍵の発行を受け、自分自身が管理している加盟店端末装置18とICカード12との間の認証処理を実行するようにしても良いことはもちろんである。

【0049】

例えば、コンビニエンスストアや駅などに設置されるMMK (Multi Media KIOSK (マルチメディアキオスク)) 20において、本サービスが提供される場合、アクワイアラ・ブランドホルダ1は、それぞれの店舗4に設置されるMMK20を統括するMMKセンタ19に対して鍵を発行して、配布する。

【0050】

マルチメディア端末の一種であるMMK 2 0は、ATM (Automatic Teller Machine) と、公共料金の収納代行やEC (Electronics Commerce (電子商取引)) 機能などを備える端末が融合した多機能型端末のことである。MMK 2 0 (図2においては、MMK 2 0を1つだけ図示しているが、実際には、複数の店舗4に、それぞれMMK 2 0が設置されている) は、MMKセンタ19と、例えば、専用線を用いて接続されており、利用者3が、本サービスの電子マネーを、MMK 2 0において利用するとき、MMK 2 0は、MMKセンタ19と接続することにより、ICカード12との認証処理を実行するが、加盟店端末装置18の場合と同様に、MMK 2 0が高度なタンパ技術を用いたものであれば、それぞれのMMK 2 0に鍵を記憶させて、MMK 2 0とICカード12との間で認証処理を実行させるようにしても良い。

【0051】

なお、MMK 2 0が、ICカード12に対する電子マネー充填サービスを行う機能を有している場合、MMKセンタ19は、対応するイシュア2に接続され、電子マネー充填サービスによって発生する課金処理に関する情報を授受することができるようになる。

【0052】

また、図2においては、MMKセンタ19をひとつだけ図示して説明しているが、複数のMMKセンタ19が、その提携内容に基づいて、アクワイアラ・ブランドホルダ1から鍵の発行を受け、自分自身が管理しているMMK 2 0とICカード12との間の認証処理を実行するようにしても良いことはもちろんである。

【0053】

統括して管理する機構がない店舗4が、単独で、本サービスと提携した場合、アクワイアラ・ブランドホルダ1は、それぞれの店舗4に設置される加盟店端末装置21に対して鍵を発行し、配布する。加盟店端末装置21は鍵を記憶し、加盟店端末装置21とICカード12との間で認証処理が実行される。

【0054】

あるいは、アクワイアラ・ブランドホルダ1と加盟店端末装置21とをオンライン化し、鍵を、加盟店端末装置21に配布せずに、アクワイアラ・ブランドホ

ルダ 1 に記録させるようにしてもよい。加盟店端末装置 2 1 は、ＩＣカード 1 2 との各種処理の開始時に、アクワイアラ・ブランドホルダ 1 に認証情報を送信し、認証処理の実行を要求するようにしても良い。この場合、トランザクション毎の処理に対するコストが発生するが、加盟店端末装置 2 1 に高度なタンパ技術を用いる必要がなくなる。

【 0 0 5 5 】

なお、図 2 においては、加盟店端末装置 2 1 をひとつだけ図示して説明しているが、複数の加盟店端末装置 2 1 が、その提携内容に基づいて、アクワイアラ・ブランドホルダ 1 から鍵の発行を受け、ＩＣカード 1 2 との間の認証処理を実行するようにしても良いことはもちろんである。

【 0 0 5 6 】

また、利用者 3 は、パーソナルコンピュータ 1 4 に接続されたリーダライタ 1 5 を用いて、ＩＣカード 1 2 との情報の授受を行わせることにより、店舗 4 に赴くことなく、インターネット 1 1 を介して、例えば、イシュア 2 - 2 と接続し、電子マネーの充填を行ったり、インターネット 1 1 上に公開されているサイバー店舗 1 6 において、商品を購入することが可能である。サイバー店舗 1 6 は、インターネット 1 1 と接続され、インターネット 1 1 上に、商品やサービスを紹介したり、販売するためのウェブコンテンツを公開し、インターネット 1 1、パーソナルコンピュータ 1 4 およびリーダライタ 1 5 を介して、ＩＣカード 1 2 との情報の授受を行うことにより、利用者 3 に各種サービスを提供できるようになされている。

【 0 0 5 7 】

サイバー店舗 1 6 は、アクワイアラ・ブランドホルダ 1 との提携により鍵の発行は受けるが、発行された鍵の供給を受けない。アクワイアラ・ブランドホルダ 1 は、サイバー店舗 1 6 に発行した鍵を自分自身に保存し、サイバー店舗 1 6 からの要求に従って、所定のＩＣカード 1 2 との認証処理を実行する。すなわち、本システムにおいては、インターネット 1 1 を介した鍵の供給は行われないうようになされている。

【 0 0 5 8 】

なお、図2においては、サイバー店舗16、パーソナルコンピュータ14およびリーダライタ15をそれぞれひとつだけ図示して説明しているが、複数のサイバー店舗16が、その提携内容に基づいて、アクワイアラ・ブランドホルダ1から鍵の発行を受け、リーダライタ15、パーソナルコンピュータ14、およびインターネット11を介してICカード12から認証情報の入力を受け、アクワイアラ・ブランドホルダ1に対して認証処理を要求することにより、利用者3に各種サービスを提供することができるようによようにしても良いことはもちろんである。

【0059】

図2を用いて説明した鍵をはじめとする情報の授受は、セキュリティを重視して、できる限り専用線を用いて通信することが望ましい。しかしながら、いずれかの接続において、インターネット11などの広域ネットワークを使用せざるを得ない場合、送受信される情報は、例えば、SSL (Secure Sockets Layer) などを用いて暗号化される。

【0060】

また、鍵を含む認証情報や、ICカード12の電子マネーの残高に関する情報などの特に重要な情報については、例えば、本システム独自の暗号化・復号ルールを制定して、それらに基づいて情報の授受がなされるようにしても良い。なお、これらの情報の通信において、インターネット11などの広域ネットワークを使用せざるを得ない場合、送受信される情報は、本システム独自のルールに基づいて暗号化され、更にSSLにより暗号化されるようにしてもよい。

【0061】

なお、アクワイアラ・ブランドホルダ1から供給される鍵は、例えば、磁気ディスク（フロッピーディスクを含む）、光ディスク（CD-ROM (Compact Disk-Read Only Memory) , DVD (Digital Versatile Disk) を含む）、光磁気ディスク（MD (Mini-Disk)を含む）、あるいは、半導体メモリなどのリムーバブルメディアに保存して、イシュア2、POSセンタ17、MMKセンタ18、もしくは加盟店端末装置21に対して配布されるようにしても良い。

【0062】

このようなシステムを構成することにより、店舗4、多くの店舗4を有する企業（例えばコンビニエンスストアなど）、あるいは、実際の販売店としての店舗4を持たないが、MMK20やインターネット11上のサイバー店舗16といった形態で事業を展開する企業などは、本システムにおいて、それぞれの事業に合致したサービスを選択して、利用者3に提供することができ、利用者3も、自分自身が享受したいサービスと提携しているICカード12を発行するイシュア2を選択して、ICカード12の発行を受けることができる。

【0063】

また、本システムは、このような自由度の高いシステムであるのにもかかわらず、電子マネーのブランド管理、および認証処理に用いられる鍵の管理が一元化されているため、システム全体としての管理・運営コストを抑えることができ、更に、セキュアな情報の授受を実現することが可能となる。

【0064】

図2を用いて説明したように、本サービスに提携しているイシュア2、POSセンタ17、MMKセンタ18、および加盟店端末装置21には、アクワイアラ・ブランドホルダ1から、その提携内容に基づいた鍵が発行され、供給される。入金端末装置13、加盟店端末装置18および21、MMK20には、それぞれ、リーダライタおよびリーダライタを制御するコントローラが含まれ、ICカード12と、非接触もしくは電氣的接触により通信が行われるようになされている。ここでは、ICカード12とリーダライタは、非接触通信を行うものとし、入金端末装置13、加盟店端末装置18および21、MMK20には、それぞれ、図3に示されるリーダライタ31およびコントローラ32が含まれているものとする。

【0065】

図3に示される非接触カードシステムにおいては、リーダライタ31とICカード12との間では、電磁波を利用して非接触でデータの送受信が行われるようになされている。すなわち、リーダライタ31が、所定のコマンドをICカード12に送信し、ICカード12は、そのコマンドを受信し、そのコマンドに対応する処理を行う。そして、ICカード12は、その処理結果に対応する応答デー

タをリーダライタ 3 1 に送信する。

【 0 0 6 6 】

リーダライタ 3 1 は、所定のインターフェース（例えば、RS-485A の規格などに準拠したもの）を介してコントローラ 3 2 に接続されており、コントローラ 3 2 は、リーダライタ 3 1 に対して所定の制御信号を供給することで、所定の処理を行わせる。

【 0 0 6 7 】

図 4 は、リーダライタ 3 1 の構成を示すブロック図である。なお、図 2 のリーダライタ 1 5 も、基本的に図 4 のリーダライタ 3 1 と同様の構成を有するものであるので、その説明は省略する。

【 0 0 6 8 】

IC 4 1 は、データの処理を行う DPU (Data Processing Unit) 5 1、IC カード 1 2 に送信するデータおよび IC カード 1 2 から受信したデータの処理を行う SPU (Signal Processing Unit) 5 2、コントローラ 3 2 との通信を行う SCC (Serial Communication Controller) 5 3、並びに、データの処理に必要な情報を予め記憶している ROM (Read Only Memory) 6 1 および処理途中のデータを一時的に記憶する RAM (Random Access Memory) 6 2 とで構成されるメモリ 5 4 により構成され、DPU 5 1 乃至メモリ 5 4 は、バス 5 5 を介して、相互に接続されている。

【 0 0 6 9 】

また、このバス 5 5 には、例えば、認証のために必要なデータ（例えば、アクワイアラ・ブランドホルダ 1 から供給された鍵など）をはじめとする、所定のデータを記憶するフラッシュメモリ 4 2、および、ドライブ 4 7 も接続されている。ドライブ 4 7 には、必要に応じて磁気ディスク 6 5、光ディスク 6 6、光磁気ディスク 6 7、および半導体メモリ 6 8 が装着され、データの授受を行う。

【 0 0 7 0 】

アンテナ 4 6 は、所定の電磁波を放射した状態で負荷状態を監視することにより、IC カード 1 2 が装着されたか否かを検出し、装着された IC カード 1 2 に対してデータの送受信を行う。IC カード 1 2 に対するデータの送受信について

の詳細は後述する。

【0071】

復調回路44は、アンテナ46を介して受信した変調波（ASK（Amplitude Shift Keying）変調波）を復調し、復調されたデータをSPU52に出力する。

【0072】

SPU52は、復調回路44を介して、ICカード12から送信された応答データの入力を受け、そのデータに対して所定の処理（例えば、BPSK（Binary Phase Shift Keying）変調（ワンチェスタコードへのコーディング）など）を施すとともに、ICカード12に送信するコマンドに対しても、同様に、所定の処理を行った後、変調回路43に出力する。

【0073】

DPU51は、SPU52およびバス55を介して、ICカード12から受信した応答データや、SCC53およびバス55を介してコントローラ32から入力される制御信号の入力を受け、入力された応答データや制御信号に従った処理を実行し、ICカード12に送信するコマンドを、バス55を介してSPU52に出力したり、コントローラ32に出力するデータを、バス55を介してSCC53に出力する。

【0074】

変調回路43は、発振器（OSC）45より供給される所定の周波数（例えば13.56MHz）の搬送波を、SPU52より供給されるデータに基づいて、ASK変調し、生成された変調波を、アンテナ46を介して、電磁波としてICカード12に出力する。なお、このとき、変調回路43は、変調度を1未満にして、ASK変調を行うようになされており、これにより、データがローレベルのときにおいても、変調波の最大振幅がゼロにならないようになされている。

【0075】

SCC53は、コントローラ32から入力されたデータを、バス55を介して、DPU51に供給したり、DPU51から、バス55を介して入力されたデータを、コントローラ32に出力する。

【0076】

図5は、図1のICカード12の構成を示すブロック図である。

【0077】

ICカード12のIC71は、アンテナ73を介して、リーダライタ31（もしくは、リーダライタ15）により送信された変調波を受信する。コンデンサ72は、アンテナ73とともにLC回路を構成し、所定の周波数（キャリア周波数）の電磁波に同調（共振）する。

【0078】

IC71のインターフェース部81は、ASK復調部91で、アンテナ73を介して受信した変調波（ASK変調波）を検波して復調し、復調後のデータを、BPSK復調部82およびPLL（Phase Locked Loop）部83に出力するとともに、電圧レギュレータ92で、ASK復調部91が検波した信号を安定化し、各回路に直流電源として供給する。また、インターフェース部81は、発振回路93でデータのクロック周波数と同一の周波数の信号を発振し、その信号をPLL部83に出力する。

【0079】

更に、ICカード12からリーダライタ31へデータを送信する場合、インターフェース部81のASK変調部94は、演算部84からBPSK変調部88を介して供給されるデータに対応して、例えば、所定のスイッチング素子をオン／オフさせ、スイッチング素子がオン状態であるときだけ所定の負荷をアンテナ73に並列に接続させることにより、ICカード12の電源としてのアンテナ73の負荷を変動させる。ASK変調部94は、アンテナ73の負荷の変動により、アンテナ73を介して受信している変調波をASK変調し（リーダライタ31は、ICカード12からデータを受信するとき、すなわち、ICカード12にデータを送信させるとき、その出力する変調波の最大振幅を一定にしており、この変調波が、アンテナ73の負荷の変動により、ASK変調される）、その変調成分を、アンテナ73を介してリーダライタ31に送信する（すなわち、リーダライタ31のアンテナ46の端子電圧を変動させる）。

【0080】

PLL部83は、ASK復調部91より供給されるデータから、そのデータに

同期したクロック信号を生成し、そのクロック信号をBPSK復調部82およびBPSK変調部88に出力する。BPSK復調部82は、ASK復調部91で復調されたデータが、BPSK変調されている場合、PLL部83より供給されたクロック信号に従って、そのデータの復調（ワンチェスタコードのデコード）を行い、復調したデータを演算部84に出力する。

【0081】

演算部84は、BPSK復調部82より供給されたデータが暗号化されている場合、そのデータを暗号／復号部96で復号化した後、そのデータを、シーケンサ95で処理する。なお、データが暗号化されていない場合、BPSK復調部82より供給されたデータは、暗号／復号部96を介さず、シーケンサ95に、直接供給される。

【0082】

シーケンサ95は、入力されるコマンドに従った各種の処理を実行する。すなわち、シーケンサ95は、例えば、EEPROM (Electrically Erasable and Programmable Read Only Memory) 86に対するデータの書き込みや読み出し、その他データに対する必要な演算処理などを行う。更に、シーケンサ95は、認証を行うことによるEEPROM86へのアクセス制御や、EEPROM86の管理などを実行する。

【0083】

演算部84のパリティ演算部97は、EEPROM86に記憶されるデータや、EEPROM86に記憶されているデータから、パリティとして、例えば、リードソロモン符号を算出する。更に、演算部84は、シーケンサ95で所定の処理を行った後、その処理に対応する応答データ（リーダライタ31に送信するデータ）をBPSK変調部88に出力する。BPSK変調部88は、演算部84より供給されたデータをBPSK変調し、変調後のデータをインターフェース部81のASK変調部94に出力する。

【0084】

ROM85は、シーケンサ95が処理を行うためのプログラム、およびプログラムの実行に必要なデータなどを記憶している。RAM87は、シーケンサ95

が処理を行うとき、その処理の途中のデータなどを、一時的に記憶する。EEPROM 86は、不揮発性のメモリであり、ICカード12が、リーダライタ31との通信を終了し、その電力供給が停止された後も、データを記憶し続ける。

【0085】

次に、リーダライタ31とICカード12との間のデータの送受信処理について説明する。

【0086】

図4を用いて説明したリーダライタ31は、アンテナ46から所定の電磁波を放射した状態で、アンテナ46の負荷状態を監視し、ICカード12が接近することによる負荷状態の変化が検出されるまで待機する。なお、リーダライタ31には、所定の短いパターンのデータでASK変調した電磁波を放射して、ICカード12への呼びかけを、ICカード12からの応答が一定時間内に得られるまで繰り返す処理（ポーリング）を行わせるようにしてもよい。

【0087】

リーダライタ31において、ICカード12の接近が検出されると、リーダライタ31のSPU52は、所定の周波数（例えば、データのクロック周波数の2倍の周波数）の矩形波を搬送波として、ICカード12に送信するデータ（例えば、ICカード12に実行させる処理に対応するコマンドや、ICカード12に書き込むデータなど）で、BPSK変調を行い、生成した変調波（BPSK変調信号）を変調回路43に出力する。

【0088】

なお、BPSK変調時においては、差動変換を利用して、変調波の位相の変化に、データを対応させることができ、この場合、BPSK変調信号が反転しても、元のデータに復調されるので、復調するときに、変調波の極性を配慮する必要がなくなる。

【0089】

変調回路43は、入力されたBPSK変調信号で、所定の搬送波を1未満（例えば0.1）の変調度（＝データ信号の最大振幅／搬送波の最大振幅）でASK変調し、生成された変調波（ASK変調波）を、アンテナ46を介してICカー

ド12に送信する。

【0090】

なお、送信を行わないとき、変調回路43は、デジタル信号の2つのレベル（ハイレベルとローレベル）のうちの、例えばハイレベルで変調波を生成するようになされている。

【0091】

図5を用いて説明したICカード12では、アンテナ73およびコンデンサ72で構成されるLC回路において、リーダライタ31のアンテナ46が放射した電磁波の一部が電気信号に変換され、その電気信号（変調波）が、IC71のインターフェース部81に出力される。そして、インターフェース部81のASK復調部91は、その変調波を整流平滑化することで、包絡線検波を行い、これにより生成される信号を電圧レギュレータ92に供給するとともに、その信号の直流成分を抑制してデータ信号を抽出し、そのデータ信号をBPSK復調部82およびPLL部83に出力する。

【0092】

なお、このとき、アンテナ73の端子電圧 V_0 は、例えば次の式（1）で表される。

$$V_0 = V_{10} (1 + k \times V_s(t)) \cos(\omega t) \dots (1)$$

但し、 $V_{10} \cos(\omega t)$ は、搬送波を、 k は変調度を、 $V_s(t)$ はSPU52が出力するデータを、それぞれ表す。

【0093】

また、ASK復調部91による整流後の電圧 V_1 におけるローレベルの値 V_{LR} は、例えば次の式（2）で表される。

$$V_{LR} = V_{10} (1 + k \times (-1)) - V_f \dots (2)$$

【0094】

ここで、 V_f は、ASK復調部91において、整流平滑化を行うための整流回路を構成するダイオード（図示せず）における電圧降下を示しており、一般に0.7ボルト程度である。

【0095】

電圧レギュレータ 9 2 は、A S K 復調部 9 1 により整流平滑化された信号を受信すると、その信号を安定化し、直流電源として、演算部 8 4 を始めとする各回路に供給する。なお、ここでは、上述したように、変調波の変調度 k は 1 未満であるので、整流後の電圧変動（ハイレベルとローレベルの差）が小さい。従って、電圧レギュレータ 9 2 において、直流電源を容易に生成することができる。

【 0 0 9 6 】

ここで、例えば、変調度 k が 5 % の変調波を、 V_{10} が 3 ボルト以上になるように受信した場合、整流後のローレベル電圧 V_{LR} は、 $2.15 (= 3 \times (1 - 0.05) - 0.7)$ ボルト以上となり、電圧レギュレータ 9 2 は、電源として十分な電圧を各回路に供給することができる。更に、この場合、整流後の電圧 V_1 の交流成分（データ成分）の振幅 $2 \times k \times V_{10}$ （Peak-to-Peak 値）は、 $0.3 (= 2 \times 0.05 \times 3)$ ボルト以上になり、A S K 復調部 9 1 は、十分高い S/N 比でデータの復調を行うことができる。

【 0 0 9 7 】

このように、変調度 k が 1 未満の A S K 変調波を利用することにより、エラーレートの低い（すなわち、 S/N 比の高い）状態での通信が実現されるとともに、電源として十分な直流電圧が I C カード 1 2 に供給される。

【 0 0 9 8 】

B P S K 復調部 8 2 は、A S K 復調部 9 1 からデータ（B P S K 変調信号）を受信すると、そのデータを、P L L 部 8 3 より供給されるクロック信号に従って復調し、復調したデータを演算部 8 4 に出力する。

【 0 0 9 9 】

演算部 8 4 は、B P S K 復調部 8 2 より供給されたデータが暗号化されている場合は、暗号／復号部 9 6 で復号化した後、そのデータをシーケンサ 9 5 に供給して処理する。なお、リーダライタ 3 1 は、この期間、すなわち、I C カード 1 2 にデータを送信後、それに対する返答を受信するまでの間、値が 1 のデータを送信したまま待機している。従って、この期間においては、I C カード 1 2 は、最大振幅が一定である変調波を受信している。

【 0 1 0 0 】

シーケンサ95は、処理が終了すると、その処理結果などについての応答データ（リーダライタ31に送信するデータ）を、BPSK変調部88に出力する。BPSK変調部88は、入力されたデータをBPSK変調（ワンチェスタコードにコーディング）した後、インターフェース部81のASK変調部94に出力する。

【0101】

そして、ASK変調部94は、アンテナ73の両端に接続される負荷を、スイッチング素子などを利用し、BPSK変調部88からのデータに応じて変動させることにより、受信している変調波（ICカード12によるデータの送信時においては、上述したように、リーダライタ31が出力する変調波の最大振幅は一定とされている）を、送信するデータに応じてASK変調し、これによりリーダライタ31のアンテナ46の端子電圧を変動させて、そのデータをリーダライタ31に送信する。

【0102】

一方、リーダライタ31の変調回路43は、ICカード12からのデータの受信時においては、値が1（ハイレベル）のデータの送信を継続している。そして、復調回路44において、ICカード12のアンテナ73と電磁氣的に結合しているアンテナ46の端子電圧の微小な変動（例えば、数十マイクロボルト）から、ICカード12により送信されたデータが検出される。

【0103】

更に、復調回路44では、検出した信号（ASK変調波）が高利得の増幅器（図示せず）で増幅されて復調され、その結果得られるデジタルデータがSPU52に出力される。SPU52は、入力されたデータ（BPSK変調信号）を復調し、バス55を介して、DPU51に出力する。DPU51は、SPU52から入力されたデータを処理し、その処理結果に応じて、通信を終了するか否かを判断する。そして、再度、通信を行うと判断された場合、上述した場合と同様に、リーダライタ31とICカード12との間で通信が行われる。一方、通信を終了すると判断された場合、リーダライタ31とICカード12との通信処理が終了される。

【0104】

以上のように、リーダライタ31は、変調度 k が1未満であるASK変調を利用して、ICカード12にデータを送信し、ICカード12は、そのデータを受け取り、そのデータに対応する処理を行って、その処理の結果に対応するデータを、リーダライタ31に返送する。

【0105】

次に、図6を用いて、図5のEEPROM86の論理フォーマットについて説明する。

【0106】

EEPROM86は、ブロックを単位として構成され、例えば、図6においては、1ブロックは、16バイトで構成されている。

【0107】

更に、図6においては、最も上のブロックの論理アドレスを#0000h (h 16進数を表す)として、昇順に、論理アドレスが付されている。なお、図6では、論理アドレスとして、#0000h乃至#FFFFhが付されており、従って、65536 ($=2^{16}$) 個のブロックが構成されている。

【0108】

それぞれのブロックは、ユーザブロックまたはシステムブロックとして使用されるようになされている。EEPROM86の各ブロックは、論理アドレスの昇順に、ユーザブロックに割り当てられていき、また、論理アドレスの降順に、システムブロックに割り当てられていくようになされている。すなわち、図6において、ユーザブロックは下方向に、システムブロックは上方向に、それぞれ増えていき、空きブロックがなくなった時点で、ユーザブロックおよびシステムブロックをつくることはできなくなる。従って、ユーザブロックとシステムブロックとの境界は固定ではなく、また、ユーザブロックの数、またはシステムブロックの数それぞれには、特に制限がない(但し、図6の場合においては、ユーザブロックとシステムブロックとの合計は、65536個以下に制限される)。

【0109】

システムブロックには、製造ID (Identification) ブロック、発行IDプロ

ック、システム定義ブロック、エリア定義ブロック、サービス定義ブロックの5種類がある。なお、図6の場合においては、エリア定義ブロックまたはサービス定義ブロックとなっているブロックを、エリア／サービス定義ブロックと示している。

【0110】

システムブロックのうち、製造IDブロック、発行IDブロック、システム定義ブロックの3つは、基本的に、ICカード12の発行時には、既に配置されているもので、論理アドレス#FFFFh、#FFFEh、#FFFDhにそれぞれ配置される。そして、エリア／サービス定義ブロックは、論理アドレス#FFFC hより上に、作成順に配置されていく。

【0111】

製造IDブロックには、ICカード12の製造に関する情報が配置される。すなわち、製造IDブロックには、例えば、ユニークな製造ID、製造年月日、あるいは製造者のコードなどが配置される。

【0112】

発行IDブロックには、ICカード12の発行に関する情報が配置される。すなわち、発行IDブロックには、例えば、ICカード12が発行された日付、ICカード12を発行した順番を表すコード、あるいは、カードIDなどが配置される。

【0113】

システム定義ブロックには、例えば、EEPROM 86が有するシステムブロックまたはユーザブロックの数や、ICカード12を発行したイシュア2が、アクワイアラ・ブランドホルダ1から配布された鍵などが配置される。この鍵は、上述したように、ICカード12と、リーダライタ31およびコントローラ32との間で、相互認証を行うときに用いられる。

【0114】

エリア定義ブロックは、例えば、EEPROM 86の記憶領域（エリア）が、本サービスをはじめとする各種サービスを実現させるための記憶領域に割り当てられることにより作成され、それらが配置された記憶領域を管理するための情報などが

配置される。すなわち、エリア定義ブロックには、例えば、本サービスに関する情報を記録する領域に対応するコード範囲、それぞれの記憶領域の空き容量などが配置される。

【 0 1 1 5 】

サービス定義ブロックには、後述する、様々なサービスを提供するためのアプリケーションが配置されているサービス領域を管理するための情報（サービス領域の容量や処理を行うために必要な鍵など）などが配置される。

【 0 1 1 6 】

次に、図 7 は、コントローラ 3 2 の構成を示すブロック図である。

【 0 1 1 7 】

制御部 1 0 1 は、内部バス 1 0 2 を介して、入力部 1 0 3 を用いて入力された各種指令に対応する信号に基づいた各種処理を実行する。メモリ 1 0 4 は、制御部 1 0 1 が使用するプログラム、演算用のパラメータ、もしくは、プログラムの実行において適宜変化するパラメータなどを格納する。制御部 1 0 1 およびメモリ 1 0 4 は、内部バス 1 0 2 により相互に接続されている。

【 0 1 1 8 】

内部バス 1 0 2 は、入力部 1 0 3、表示部 1 0 5、ドライブ 1 0 6、およびネットワークインターフェース 1 0 7 とともに接続されている。入力部 1 0 3 は、例えば、キーボード、マウスあるいはバーコードリーダなどからなり、制御部 1 0 1 に各種の指令、あるいはデータなどを入力するとき操作される。表示部 1 0 5 は、例えば、CRT (Cathode Ray Tube) 等からなり、各種情報をテキスト、もしくはイメージなどで表示する。ドライブ 1 0 6 には、必要に応じて磁気ディスク 1 1 1、光ディスク 1 1 2、光磁気ディスク 1 1 3、および半導体メモリ 1 1 4 が装着され、データの授受を行う。

【 0 1 1 9 】

ネットワークインターフェース 1 0 7 は、例えば、RS-485A を介して、リーダライタ 3 1 に接続されたり、所定のインターフェースケーブルなどを用いて LAN (Local Area Network) に接続されたり、図示しない電話回線などを介して、例えばインターネット 1 1 などの広域ネットワークに接続される。

【0120】

また、図2を用いて説明したように、リーダライタ15を、パーソナルコンピュータ14と接続させることにより、利用者3は、店舗に赴くことなく、ICカード12を用いた本サービスを楽しむことが可能となる。図8は、パーソナルコンピュータ14の構成を示すブロック図である。

【0121】

CPU121は、入出力インターフェース122および内部バス123を介して、例えば、利用者3が入力部124を用いて入力した各種指令に対応する信号や、ネットワークインターフェース125を介して入力された信号を受け、それらの信号に基づいた各種処理を実行する。ROM126は、CPU121が使用するプログラム（例えば、インターネット11に公開されているウェブコンテンツを閲覧するためのウェブブラウザなど）や、演算用のパラメータのうちの基本的に固定のデータを格納する。RAM127は、CPU121の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。CPU121、ROM126、およびRAM127は、内部バス123により相互に接続されている。

【0122】

内部バス123は、入出力インターフェース122とも接続されている。入力部124は、例えば、キーボードやマウスからなり、CPU121に各種の指令を入力するとき操作される。表示部128は、例えば、CRT（Cathode Ray Tube）等からなり、各種情報をテキスト、あるいはイメージなどで表示する。HDD（Hard Disk Drive）129は、ハードディスクを駆動し、CPU121が使用するプログラムや、それらのプログラムの処理により生成されたデータを記録または再生させる。ドライブ130には、必要に応じて磁気ディスク131、光ディスク132、光磁気ディスク133、および半導体メモリ134が装着され、データの授受を行う。ネットワークインターフェース125は、図示しない電話回線などを介してインターネット11と接続され、また、所定の接続ケーブルを用いて、リーダライタ15と接続され、情報の授受を行う。

【0123】

また、図2を用いて説明したPOSセンタ17およびMMKセンタ19も、図8のパーソナルコンピュータ14と、基本的に、同様の構成を有するので、その説明は省略する。

【0124】

図9は、アクワイアラ・ブランドホルダ1の構成を示すブロック図である。なお、店舗管理サーバ141乃至 이슈アG/W（ゲートウェイ）サーバ151の内部構成は、基本的に、図8を用いて説明したパーソナルコンピュータ14と同様であるので、その説明は省略する。

【0125】

店舗管理サーバ141は、本サービスと提携している 이슈ア2および店舗4に関する情報を記録する店舗管理DB（データベース）142を管理するサーバであり、店舗管理DB142には、例えば、本サービスと提携している 이슈ア2および店舗4の名称、住所、対応する 이슈ア2もしくは店舗4との清算処理に利用される金融機関の口座番号、本サービスにおける提携内容、および発行された鍵に対応する鍵IDなどが記録されている。

【0126】

顧客サーバ142は、本サービスを享受している利用者3（すなわち、アクワイアラ・ブランドホルダ1が管理している電子マネーブランドのサービスの利用者）に関する情報を記録する顧客DB144を管理するサーバであり、顧客DB144には、例えば、顧客の氏名、住所、対応する顧客が有する金融機関の口座番号もしくはクレジットカードのカード番号など、顧客が清算処理に利用する金融機関の情報、および、顧客が保有するICカード12のカードIDなどが記録されている。

【0127】

セキュリティサーバ145は、本サービスにおいて利用される全ての鍵に関する情報、並びに、それぞれの鍵の発行（配布）先となる 이슈ア2もしくは店舗4などに関する情報を記録する鍵管理DB146を管理するためのサーバであり、必要に応じて、新たに提携された 이슈ア2、もしくは、店舗4に対して発行すべき鍵を検索し、 이슈アG/Wサーバ151、もしくは、店舗G/Wサー

バ149に出力する。

【0128】

課金サーバ147は、店舗G/Wサーバ149、もしくは、ウェブサーバ150から入力される、提携している店舗からの課金情報を基に、課金処理を行い、イシュア2に対する請求金額を算出し、イシュアG/Wサーバ151を介して、対応するイシュア2に出力する。課金処理は、例えば、1週間、1ヶ月などの所定の期間毎に行うようにしても良い。更に、課金サーバは、図14および図16を用いて後述する、イシュア2-1が発行したICカード12に対する電子マネーの充填代行サービスに関する処理も実行し、代行による入金に関する情報を入金代行DB148に記録し、例えば、1週間、1ヶ月などの所定の期間毎に、対応するイシュア2-1との清算処理を行う。

【0129】

店舗G/Wサーバ149は、図2を用いて説明したPOSセンタ17、MMKセンタ19、および加盟店端末装置21と接続され、POSセンタ17、MMKセンタ19、および加盟店端末装置21との情報の授受を制御し、入力されたデータを、店舗管理サーバ141乃至課金サーバ147の対応するサーバに出力する（例えば、POSセンタ17から、課金情報が入力された場合、入力されたデータを、課金サーバ147に出力する）サーバである。

【0130】

ウェブサーバ150は、インターネット11と接続され、サイバー店舗16もしくはパーソナルコンピュータ14との情報の授受を制御し、入力されたデータを、店舗管理サーバ141乃至課金サーバ147の対応するサーバに出力する（例えば、サイバー店舗16から、ICカード12の認証情報が入力された場合、入力されたデータを、セキュリティサーバ145に出力する）サーバである。

【0131】

イシュアG/Wサーバ151は、イシュア2と接続され、イシュア2との情報の授受を制御し、入力されたデータを、店舗管理サーバ141乃至課金サーバ147の対応するサーバに出力する（例えば、イシュア2から、新たなサービスに対応する鍵の発行要求が入力された場合、入力されたデータを、セキュリティサ

ーバ145に出力する)サーバである。

【0132】

図10は、イシュー2-1の構成を示すブロック図である。

【0133】

セキュリティサーバ161は、アクワイアラ・ブランドホルダ1から発行された鍵を保存する鍵管理DB162を管理し、ICカード12発行時に、鍵管理DB162から、必要な鍵を検索して出力したり、店舗G/Wサーバ166に接続されている入金端末装置13から入力されたICカード12の認証情報を基に、対応する鍵を鍵管理DB162から検索して認証処理を行い、認証処理結果を店舗G/Wサーバ166に出力する。

【0134】

利用者管理サーバ163は、発行したICカード12を利用する利用者3に関する情報を記録する利用者DB164を管理するサーバであり、利用者登録/ICカード発行用の図示しない処理装置などと接続されている。利用者管理サーバ163は、利用者登録/ICカード発行用の図示しない処理装置から、例えば、顧客の氏名、住所、対応する顧客が有する金融機関の口座番号もしくはクレジットカードのカード番号、顧客が清算処理に利用する金融機関の情報、および、顧客が保有するICカード12のカードIDなどの入力を受け、利用者DB164に記録し、セキュリティサーバ161から出力された鍵を、利用者登録/ICカード発行用の処理装置に出力する。

【0135】

アクワイアラ・ブランドホルダG/Wサーバ165は、アクワイアラ・ブランドホルダ1と接続され、情報の授受を制御し、入力されたデータを、セキュリティサーバ161乃至課金サーバ167の対応するサーバに出力する(例えば、アクワイアラ・ブランドホルダ1から、新たなサービスに対応する鍵が発行され、入力された場合、入力された鍵を、セキュリティサーバ161に出力する)。

【0136】

店舗G/Wサーバ166は、図2を用いて説明した入金端末装置13、もしくは、MMKセンタ19と接続され、入金端末装置13、もしくは、MMKセンタ

19との情報の授受を制御し、入力されたデータを、セキュリティサーバ161乃至課金サーバ167の対応するサーバに出力する。例えば、入金端末装置13から、ICカード12に対する電子マネーの充填処理に関する情報が入力された場合、入力されたデータを、課金サーバ167に出力し、入金端末装置13から、ICカード12に関する認証情報が入力された場合、入力されたデータをセキュリティサーバ161に出力する。

【0137】

課金サーバ167は、店舗G/Wサーバ166から入力される入金端末装置13、もしくは、MMKセンタ19からの課金情報を基に、ICカード12への電子マネーの充填処理に関する課金処理を行い、課金処理結果を、入金DB168に記録する。

【0138】

図11は、イシュア2-2の構成を示すブロック図である。なお、図10のイシュア2-1と対応する部分には同一の符号を付してあり、その説明は適宜省略する（以下、同様）。

【0139】

ウェブサーバ171は、インターネット11と接続され、情報の授受を制御し、入力されたデータを、セキュリティサーバ161乃至課金サーバ167の対応するサーバに出力する（例えば、パーソナルコンピュータ14から、ICカード12の認証情報が入力された場合、入力されたデータを、セキュリティサーバ161に出力する）サーバである。

【0140】

また、課金サーバ168は、店舗G/Wサーバ166のみならず、ウェブサーバ171から入力される、パーソナルコンピュータ14からの電子マネー充填要求に基づいて、ICカード12への電子マネーの充填処理に関する課金処理を行い、課金処理結果を、入金DB168に記録する。

【0141】

次に、図12乃至図16を用いて、ICカード12への電子マネーの充填処理と、電子マネーの充填処理を実行するための鍵の配置の詳細について説明する。

【0142】

まず、図12を用いて、利用者3が、実際の店舗などに赴いて、入金端末装置13もしくはMMK20を利用して、ICカード12への電子マネーの充填処理を行うことができるようにするための鍵の配置について説明する。

【0143】

アクワイアラ・ブランドホルダ1は、例えば、ICカード12に対して、データの書き込み（すなわち、電子マネーの充填処理）を実行することを認証する鍵A乃至Cを有するものとする。例えば、鍵Aによって、A信販会社のキャッシングサービスによる電子マネーの充填処理ができ、鍵Bによって、B銀行の口座からの引き落としによる電子マネーの充填処理ができ、鍵Cによって、クレジットカードCによる電子マネーの充填処理ができるものとする。

【0144】

そして、イシュア2-3と銀行センタ181との契約により、銀行センタ181が管理する入金端末装置13において、A信販会社のキャッシングサービスおよびB銀行の口座からの引き落としによる電子マネーの充填処理を行うことができるようにするために、鍵Aおよび鍵Bが必要であるものとする。その場合、アクワイアラ・ブランドホルダ1は、イシュア2-3に対して、銀行センタ181に、対応する鍵を発行してよいか否かを確認し、イシュア2-3の許可を得て、銀行センタ181に鍵Aおよび鍵Bを発行して配布する。

【0145】

なお、銀行センタ181は、図8を用いて説明したパーソナルコンピュータ14と、基本的に、同様の構成を有するので、その説明は省略する。

【0146】

同様に、イシュア2-4とMMKセンタ19との契約により、MMKセンタ19が管理するMMK20において、A信販会社のキャッシングサービスおよびクレジットカードCによる電子マネーの充填処理を行うことができるようにするために、鍵Aおよび鍵Cが必要であるものとする。その場合、アクワイアラ・ブランドホルダ1は、イシュア2-4に対して、MMKセンタ19に、対応する鍵を発行してよいか否かを確認し、イシュア2-4の許可を得て、MMKセンタ19

に鍵Aおよび鍵Cを発行して、配布する。

【0147】

すなわち、イシュア2-3が発行したICカード12に、鍵Aおよび鍵Bが記録されている場合、そのICカード12の利用者3は、MMK20において、A信販会社のキャッシングサービスによる電子マネーの充填処理を行うことは可能であるが、B銀行の口座からの引き落としによる電子マネーの充填処理を行うことはできない。同様に、イシュア2-4が発行したICカード12に、鍵Aおよび鍵Cが記録されている場合、そのICカード12の利用者3は、銀行センタ181が管理する入金端末装置13において、A信販会社のキャッシングサービスによる電子マネーの充填処理を行うことは可能であるが、クレジットカードCによる電子マネーの充填処理を行うことはできない。

【0148】

これらの電子マネー充填処理に伴う、手数料などの清算方法は、従来の清算処理の考え方と同様に、例えば、アクワイアラ・ブランドホルダ1とイシュア2-3、アクワイアラ・ブランドホルダ1とイシュア2-4、イシュア2-3と銀行センタ181、および、イシュア2-4とMMKセンタ19とのそれぞれの提携内容に基づいて、個別に設定可能なようにしても良いし、本サービスの管理者（すなわち、アクワイアラ・ブランドホルダ1の管理者）が、アクワイアラ・ブランドホルダ1の課金サーバ147の処理により管理するようにしても良い。

【0149】

なお、図12においては、銀行センタ181に1つの入金端末装置13が接続され、MMKセンタ19に1つのMMK20が接続されているものとして説明されているが、銀行センタ181およびMMKセンタ19には、複数の入金端末装置13およびMMK20を接続することができる。また、本サービスには、複数の銀行センタ181およびMMKセンタ19が参画可能であることは言うまでもない。

【0150】

図13のフローチャートを参照して、入金端末装置13（もしくは、MMK20）を用いたICカード12への電子マネー充填処理について説明する。ここで

は、入金端末装置 1 3 を用いた I C カード 1 2 への電子マネー充填処理として説明するが、MMK 2 0 を用いた I C カード 1 2 への電子マネー充填処理を実行する場合においても、基本的に同様の処理が実行される。

【 0 1 5 1 】

ステップ S 1 において、入金端末装置 1 3 のリーダライタ 3 1 のアンテナ 4 6 は、所定の電磁波を放射した状態で負荷状態を監視することにより、I C カード 1 2 を検出し、D P U 5 1 は、I C カード 1 2 を検出したことを示す信号を生成し、バス 5 5 および S C C 5 3 を介してコントローラ 3 2 に出力する。

【 0 1 5 2 】

ステップ S 2 において、コントローラ 3 2 の制御部 1 0 1 は、ネットワークインターフェース 1 0 7 および内部バス 1 0 2 を介して、リーダライタ 3 1 から送信された I C カード 1 2 を検出したことを示す信号の入力を受け、利用者 3 に次の操作を促すためのメッセージなどを含むメニュー画面に対応するデータを、内部バス 1 0 2 を介して、表示部 1 0 5 に出力して、メニュー画面を表示させる。

【 0 1 5 3 】

ステップ S 3 において、コントローラ 3 2 の制御部 1 0 1 は、内部バス 1 0 2 を介して、入力部 1 0 3 を用いて利用者 3 が入力したコマンド（例えば、5 0 0 0 円分の電子マネー充填処理を指令するコマンド）の入力を受け、内部バス 1 0 2 およびネットワークインターフェース 1 0 7 を介して、リーダライタ 3 1 に出力し、リーダライタ 3 1 は、所定の処理を実行して、入力されたコマンドを I C カード 1 2 に送信する。

【 0 1 5 4 】

ステップ S 4 において、I C カード 1 2 のアンテナ 7 3 は、リーダライタ 3 1 より、変調波を受信し、インターフェース部 8 1、B P S K 復調部 8 2、および演算部 8 4 において所定の処理が実行され、受信されたコマンドに対応する鍵を含む認証情報が、EEPROM 8 6 から読み出される。読み出された認証情報は、演算部 8 4、B P S K 変調部 8 8、およびインターフェース部 8 1 において所定の処理を施され、アンテナ 7 3 を介して、リーダライタ 3 1 に送出される。

【 0 1 5 5 】

ステップS5において、リーダライタ31のアンテナ46は、ICカード12から送信された認証情報を受信して、復調回路44に出力する。復調回路44において復調された認証情報は、SPU52において、BPSK変調などの所定の処理を施され、DPU51に供給される。DPU51は、認証処理を依頼するための信号を生成して、入力された認証情報およびステップS3において入力された、利用者3の指令を示すコマンドとともに、バス55およびSCC53を介して、コントローラ32へ出力する。コントローラ32の制御部101は、ネットワークインターフェース107および内部バス102を介して、認証処理を依頼するための信号、利用者3の指令を示すコマンド、および認証情報の入力を受け、内部バス102およびネットワークインターフェース107を介して、対応する銀行センタ181に送信する。

【0156】

ステップS6において、銀行センタ181のCPU121（図8は、パーソナルコンピュータ14のみならず、POSセンタ17、MMKセンタ19、もしくは銀行センタ181の構成も示す図である）は、ネットワークインターフェース125、入出力インターフェース122および内部バス123を介して入力された認証処理依頼および認証情報に基づいて、アクワイアラ・ブランドホルダ1から供給され、RAM127もしくはHDD129に保存している鍵を読み出して、認証処理を行う。

【0157】

ステップS7において、銀行センタ181のCPU121は、ステップS6において実行された認証処理において、ステップS1において検出されたICカード12は、正しく認証されたか否かを判断する。ステップS7において、ICカード12は正しく認証されなかったと判断された場合、処理は、ステップS16に進む。

【0158】

ステップS7において、ICカード12は正しく認証されたと判断された場合、ステップS8において、銀行センタ181のCPU121は、入力されたコマンドを基に、利用者3が指示した方法（例えば、所定のクレジットカードによる

電子マネー 5000 円分の充填など)での価値充填処理、すなわち、ICカード 12 に記録されている電子マネーの残額の加算処理は可能か否かを確認する。銀行センタ 181 の CPU 121 は、例えば、現金による価値の充填が行われる場合、入金端末装置 13 に対して、正しい金額の現金が入金されたか否かを確認し、クレジットカードもしくは銀行口座からの引き落としによる価値の充填が行われる場合、イシュア 2 に対して、電子マネー充填分に対応するクレジットカード利用可能金額の残高、もしくは、銀行口座の残高があるか否かの問い合わせを行う。イシュア 2 は、例えば、クレジットカード会社や銀行などの所定の金融機関 5 に対して、対応する利用者 3 は、価値充填処理に対応する金額のクレジットカード利用、もしくは口座引き落としが可能か否かを問い合わせる。

【0159】

ステップ S9 において、銀行センタ 181 の CPU 121 は、ネットワークインターフェース 125、入出力インターフェース 122 および内部バス 123 を介して、入金端末装置 13、もしくはイシュア 2 から入力される、問い合わせに対するレスポンス信号を基に、価値充填処理は可能か否かを判断する。ステップ S9 において、価値充填処理ができないと判断された場合、処理は、ステップ S16 に進む。

【0160】

ステップ S9 において、価値充填処理が可能であると判断された場合、価値充填処理が可能であることを示す信号の入力を受けた入金端末装置 13 のコントローラ 32 の制御部 101 は、ステップ S10 において、価値充填処理が可能であることを示す信号を、内部バス 102 およびネットワークインターフェース 103 を介して、リーダライタ 31 に送信する。リーダライタ 31 の DPU 51 は、SCC 53 およびバス 55 を介して入力された信号を基に、価値充填処理を実行させる (ICカード 12 の対象となるファイルに記録されている電子マネーの値を書き換える) ためのコマンドを、バス 55 を介して SPU 52 に出力する。SPU 52 は、入力されたコマンドに対して、例えば、BPSK 変調などの所定の処理を行った後、変調回路 43 に出力する。変調回路 43 は、発振器 45 より供給される所定の周波数の搬送波を、SPU 52 より供給されるデータに基づいて

A S K変調し、生成された変調波を、アンテナ46を介して、電磁波としてI Cカード12に出力する。

【0161】

ステップS11において、I Cカード12のアンテナ73は、リーダライタ31のアンテナ46より、変調波を受信する。そして、受信された変調波は、インターフェース部81で検波されてA S K復調され、B P S K復調部82でB P S K復調され、演算部84の暗号／復号部96で復号され、シーケンサ95によってEEPROM86に記録されたデータの書き換え、すなわち、価値充填処理が実行され、結果が保存される。

【0162】

ステップS12において、入金端末装置13のコントローラ32の制御部101は、内部バス102およびネットワークインターフェース107を介して、銀行センタ181に処理結果を通知する。

【0163】

ステップS13において、銀行センタ181のCPU121は、ネットワークインターフェース125、入出力インターフェース122および内部バス123を介して、入金端末装置13から、価値充填処理結果の入力を受け、内部バス123、入出力インターフェース122およびネットワークインターフェース125を介して、イシュア2に処理結果を通知する。イシュア2は、入力された処理結果を、課金サーバ167の処理により、入金DB168に記録し、必要に応じて、アクワイアラ・ブランドホルダ1に、処理結果を通知する。なお、価値充填処理結果の通知は、処理が行われる毎に逐次通知するようにしても良いし、例えば1週間や1ヶ月といった、所定の期間毎に行われるようにしても良い。

【0164】

ステップS14において、入金端末装置13のコントローラ32の制御部101は、価値充填処理結果のログをI Cカード12に記録させるための制御信号を生成して、内部バス102およびネットワークインターフェース107を介して、リーダライタ31に送信し、リーダライタ31のDPU51は、SCC53およびバス55を介して入力された信号を基に、I Cカード12に送信するコマン

ドを、バス 5 5 を介して S P U 5 2 に出力する。S P U 5 2 および変調回路 4 3 で所定の処理がなされたコマンドは、アンテナ 4 6 を介して、電磁波として I C カード 1 2 に出力される。

【 0 1 6 5 】

ステップ S 1 5 において、I C カード 1 2 のアンテナ 7 3 は、リーダライタ 3 1 より、変調波を受信する。そして、インターフェース部 8 1、B P S K 復調部 8 2、および演算部 8 4 において所定の処理が実行され、EEPROM 8 6 にログが書き込まれて、保存される。

【 0 1 6 6 】

ステップ S 7 において、I C カード 1 2 が正しく認証されなかったと判断された場合、もしくは、ステップ S 9 において、価値充填処理が可能ではないと判断された場合、ステップ S 1 6 において、銀行センタ 1 8 1 の C P U 1 2 1 は、内部バス 1 2 3、入出力インターフェース 1 2 2 およびネットワークインターフェース 1 2 5 を介して、入金端末装置 1 3 に、エラーメッセージを出力する。

【 0 1 6 7 】

ステップ S 1 7 において、入金端末装置 1 3 のコントローラ 3 2 の制御部 1 0 1 は、入力されたエラーメッセージを、内部バス 1 0 2 を介して表示部 1 0 5 に出力して、表示させる。

【 0 1 6 8 】

次に、図 1 4 を用いて、利用者 3 が、実際の店舗などに赴くことなく、インターネット 1 1 を介して、I C カード 1 2 への電子マネーの充填処理を行うことができるようにするための鍵の配置、および認証処理について説明する。

【 0 1 6 9 】

アクワイアラ・ブランドホルダ 1 は、例えば、I C カード 1 2 に対するデータの書き込み（すなわち、電子マネーの充填処理）の実行を認証する鍵 D および鍵 E を有するものとする。例えば、鍵 D によって、D 信販会社のキャッシングサービスによる電子マネーの充填処理ができ、鍵 E によって、E 銀行の口座からの引き落としによる電子マネーの充填処理ができるものとする。

【 0 1 7 0 】

そして、イシュア2-2が発行するICカード12を保有する利用者3が、パーソナルコンピュータ14-1乃至14-nを用いて、D信販会社のキャッシングサービスを利用して、インターネット11を介して、電子マネーの充填処理を行うことができるようにするために、鍵Dが必要であるものとする。その場合、アクワイアラ・ブランドホルダ1は、イシュア2-2に鍵Dを発行し、配布する。イシュア2-2は、インターネット11と接続され、リーダライタ15、パーソナルコンピュータ14およびインターネット11を介して入力される、利用者3が有するICカード12の認証情報と、アクワイアラ・ブランドホルダ1から供給された鍵Dを用いて、認証処理を行い、正しく認証処理が行えた場合、電子マネーの充填処理を行う。

【0171】

また、イシュア2-1が発行するICカード12を保有する利用者3が、パーソナルコンピュータ14-1乃至14-nを用いて、E銀行の口座からの引き落としを利用して、インターネット11を介して、電子マネーの充填処理を行うことができるようにするために、鍵Eが必要であるものとする。その場合、アクワイアラ・ブランドホルダ1は、イシュア2-1に鍵Eを発行し、配布するが、イシュア2-1は、インターネット11と接続されていないため、アクワイアラ・ブランドホルダ1に対して、入金代行処理を依頼する。アクワイアラ・ブランドホルダ1は、イシュア2-1に対して発行した鍵Eを、入金代行処理用の鍵として、鍵管理DB146に記録する。

【0172】

アクワイアラ・ブランドホルダ1は、リーダライタ15、パーソナルコンピュータ14およびインターネット11を介して入力される、利用者3が有するICカード12の認証情報と、鍵管理DB146に記録された鍵Eの情報により、認証処理を行い、正しく認証処理された場合、課金サーバ147の処理により、電子マネーの充填処理を行い、その結果を入金代行DB148に記録する。

【0173】

この場合においても、電子マネー充填処理に伴う、手数料などの清算方法は、従来の清算処理の考え方と同様に、例えば、アクワイアラ・ブランドホルダ1と

イシュア 2-1、アクワイアラ・ブランドホルダ 1 とイシュア 2-2 とのそれぞれの提携内容に基づいて、個別に設定可能なようにしても良いし、本サービスの管理者（すなわち、アクワイアラ・ブランドホルダ 1 の管理者）が、アクワイアラ・ブランドホルダ 1 の課金サーバ 147 の処理により管理するようにしても良い。

【0174】

次に、図 15 のフローチャートを参照して、イシュア 2-2 による、インターネット 11 を介した IC カード 12 への電子マネー充填処理について説明する。

【0175】

パーソナルコンピュータ 14 の CPU 121 は、ステップ S21 において、入出力インターフェース 122 および内部バス 123 を介して入力部 124 から入力される、利用者 3 の操作を示す信号を基に、HDD 129 に保存されているウェブブラウザソフトウェアを RAM 127 にロードして起動させ、ウェブブラウザを立ち上げ、ステップ S22 において、インターネット 11 を介して、イシュア 2-2 に接続する。

【0176】

ステップ S23 において、イシュア 2-2 のウェブサーバ 171 は、インターネット 11 を介して、パーソナルコンピュータ 14 に、入金希望画面に対応するデータを出力する。

【0177】

ステップ S24 において、パーソナルコンピュータ 14 の CPU 121 は、ネットワークインターフェース 125、入出力インターフェース 122、および内部バス 123 を介して入力された入金希望画面に対応するデータを、内部バス 123 および入出力インターフェース 122 を介して、表示部 182 に出力して、入金希望画面を表示させる。入金希望画面には、リーダライタ 15 と IC カード 12 が通信可能な状態となるように、IC カード 12 を所定の読み取り位置に設置することを促すためのメッセージ、および、操作の入力を促すメニューなどが表示される。ここでは、IC カード 12 への価値充填処理が利用者 3 によって選択され、入力部 124 を用いて指示されたものとする。

【0178】

ステップS25において、リーダライタ15のアンテナ46は、所定の電磁波を放射した状態で負荷状態を監視することにより、ICカード12を検出し、DPU51は、ICカード12を検出したことを示す信号を生成し、バス55およびSCC53を介してパーソナルコンピュータ14に出力する。

【0179】

ステップS26において、リーダライタ15のSCC53は、パーソナルコンピュータ14より、利用者3が入力したコマンドの入力を受け、バス55を介して、SPU52に出力し、SPU52および変調回路43で所定の処理がなされたコマンドは、アンテナ46を介して、ICカード12に送信される。

【0180】

ステップS27において、図13のステップS4と同様の処理が実行される。

【0181】

ステップS28において、リーダライタ15のアンテナ46は、ICカード12から送信された認証情報を受信して、復調回路44に出力する。復調回路44において復調されたデータは、SPU52で、BPSK変調などの所定の処理を施され、DPU51に供給される。DPU51は、認証処理を依頼するための信号を生成して、入力された認証情報とともに、バス55およびSCC53を介して、パーソナルコンピュータ14に送信する。

【0182】

ステップS29において、パーソナルコンピュータ14のCPU121は、ネットワークインターフェース125、入出力インターフェース122、および内部バス123を介して、認証処理依頼および認証情報の入力を受け、利用者3が実行した操作に対応するコマンド（ここでは、ICカード12への価値充填処理を指令するためのコマンド）とともに、インターネット11を介して、イシュー2-2に送信する。

【0183】

ステップS30において、イシュー2-2のウェブサーバ171は、認証処理依頼および認証情報の入力を受け、セキュリティサーバ161に出力する。セキ

セキュリティサーバ 1 6 1 は、入力された認証処理依頼および認証情報に基づいて、自分自身がアクワイアラ・ブランドホルダ 1 から供給され、鍵管理 DB 1 6 2 に保存している鍵との認証処理を行う。

【 0 1 8 4 】

ステップ S 3 1 において、セキュリティサーバ 1 6 1 は、ステップ S 3 0 で実行された認証処理において、ステップ S 2 5 において検出された IC カード 1 2 は、正しく認証されたか否かを判断する。ステップ S 3 1 において、IC カード 1 2 は正しく認証されなかったと判断された場合、処理は、ステップ S 4 1 に進む。

【 0 1 8 5 】

ステップ S 3 1 において、IC カード 1 2 は正しく認証されたと判断された場合、ステップ S 3 2 において、課金サーバ 1 6 7 は、入力されたコマンドを基に、利用者 3 が指示した方法（例えば、所定のクレジットカードによる電子マネー 5 0 0 0 円分の充填）での価値充填処理は可能か否か（例えば、電子マネー充填分に対応するクレジット利用可能金額の残高があるか否か）を、所定の金融機関 5（クレジットカード会社、あるいは銀行など）に問い合わせることにより、確認する。

【 0 1 8 6 】

ステップ S 3 2 において、課金サーバ 1 6 7 は、金融機関 5 から送信された問い合わせに対するレスポンス信号を基に、価値充填処理は可能か否かを判断する。ステップ S 3 2 において、価値充填処理ができないと判断された場合、処理は、ステップ S 4 1 に進む。

【 0 1 8 7 】

ステップ S 3 3 において、価値充填処理が可能であると判断された場合、イシユア 2 - 2 から、インターネット 1 1、パーソナルコンピュータ 1 4 を介して、価値充填処理が可能であることを示す信号の入力を受けたリーダライタ 1 5 の D P U 5 1 は、ステップ S 3 4 において、入力された信号を基に、IC カード 1 2 に送信する、電子マネー充填処理を実行させるためのコマンドを生成して、バス 5 5 を介して S P U 5 2 に出力する。そして、S P U 5 2 および変調回路 4 3 に

において所定の処理が実行されてコマンドに対応する変調波が生成され、アンテナ 46 を介して、電磁波として IC カード 12 に出力される。

【0188】

ステップ S35 において、IC カード 12 のアンテナ 73 は、リーダライタ 15 のアンテナ 46 より、変調波を受信する。そして、インターフェース部 81、BPSK 復調部 82、および演算部 84 において所定の処理が実行され、コマンドに基づいて、EEPROM 86 に記録されたデータの書き換え、すなわち、価値充填処理が実行され、結果が保存される。

【0189】

ステップ S36 において、リーダライタ 15 の DPU 51 は、バス 55、SCC 53、パーソナルコンピュータ 14、およびインターネット 11 を介して、 이슈ア 2-2 に処理結果を通知する。

【0190】

ステップ S37 において、 이슈ア 2-2 のウェブサーバ 171 は、リーダライタ 15 から、価値充填処理結果の入力を受け、課金サーバ 167 に供給する。課金サーバ 167 は、入力された価値充填処理結果を、入金 DB 168 に記録する。

【0191】

ステップ S38 において、アクワイアラ・ブランドホルダ G/W サーバ 165 は、アクワイアラ・ブランドホルダ 1 に、価値充填処理の結果を通知する。なお、価値充填処理結果の通知は、処理が行われる毎に逐次通知するようにしても良いし、例えば、1 週間や 1 ヶ月といった、所定の期間毎に行われるようにしても良い。

【0192】

ステップ S39 において、リーダライタ 15 の DPU 51 は、SCC 53 およびバス 55 を介して入力された信号を基に、価値充填処理結果のログを IC カード 12 に記録させるためのコマンドを生成して、バス 55 を介して SPU 52 に出力する。SPU 52 および変調回路 43 で所定の処理がなされたコマンドは、アンテナ 46 を介して、電磁波として IC カード 12 に出力される。

【0193】

ステップS40において、図13のステップS15と同様の処理が実行される。

【0194】

ステップS31において、ICカード12が正しく認証されなかったと判断された場合、もしくは、ステップS33において、価値充填処理が可能ではないと判断された場合、ステップS41において、イシュー2-2のウェブサーバ171は、インターネット11を介して、パーソナルコンピュータ14に、エラーメッセージを出力する。

【0195】

ステップS42において、パーソナルコンピュータ14のCPU121は、ネットワークインターフェース125、入出力インターフェース122、および内部バス123を介して、エラーメッセージの入力を受け、内部バス123、入出力インターフェース122を介して、入力されたエラーメッセージを表示部128に出力して表示させる。

【0196】

次に、図16のフローチャートを参照して、アクワイアラ・ブランドホルダ1の入金代行による、ICカード12への電子マネー充填処理について説明する。

【0197】

ステップS51において、図15のステップS21と同様の処理が実行される。

【0198】

ステップS52において、パーソナルコンピュータ14のCPU121は、インターネット11を介して、アクワイアラ・ブランドホルダ1に接続する。

【0199】

ステップS53において、アクワイアラ・ブランドホルダ1のウェブサーバ150は、インターネット11を介して、パーソナルコンピュータ14に、入金希望画面に対応するデータを出力する。

【0200】

ステップ S 5 4 乃至ステップ S 5 8 において、図 1 5 のステップ S 2 4 乃至ステップ S 2 8 と同様の処理が実行される。

【0201】

ステップ S 5 9 において、パーソナルコンピュータ 1 4 の CPU 1 2 1 は、ネットワークインターフェース 1 2 5、入出力インターフェース 1 2 2、および内部バス 1 2 3 を介して、認証処理依頼および認証情報の入力を受け、利用者 3 が実行した操作に対応するコマンド（ここでは、ICカード 1 2 への価値充填処理を指令するコマンド）とともに、インターネット 1 1 を介して、アクワイアラ・ブランドホルダ 1 に送信する。

【0202】

ステップ S 6 0 において、アクワイアラ・ブランドホルダ 1 のウェブサーバ 1 5 0 は、認証処理依頼および認証情報の入力を受け、セキュリティサーバ 1 4 5 に出力する。セキュリティサーバ 1 4 5 は、入力された認証処理依頼および認証情報に基づいて、鍵管理 DB 1 4 6 に保存している鍵を読み出して、認証処理を行う。

【0203】

ステップ S 6 1 において、セキュリティサーバ 1 4 5 は、ステップ S 6 0 の認証処理において、ステップ S 5 5 において検出された ICカード 1 2 は、正しく認証されたか否かを判断する。ステップ S 6 1 において、ICカード 1 2 は正しく認証されなかったと判断された場合、処理は、ステップ S 7 1 に進む。

【0204】

ステップ S 6 1 において、ICカード 1 2 は正しく認証されたと判断された場合、ステップ S 6 2 において、課金サーバ 1 4 5 は、入力されたコマンドを基に、利用者 3 が指示した方法（例えば、所定のクレジットカードによる電子マネー 5000 円分の充填）での価値充填処理は可能か否か（例えば、電子マネー充填分に対応するクレジット利用可能金額の残高があるか否か）を、対応するイシューア 2-1 に問い合わせることにより、確認する。

【0205】

ステップ S 6 3 において、課金サーバ 1 4 7 は、イシューア 2-1 から送信され

た問い合わせに対するレスポンス信号を基に、価値充填処理は可能か否かを判断する。ステップS63において、価値充填処理ができないと判断された場合、処理は、ステップS71に進む。

【0206】

ステップS63において、価値充填処理が可能であると判断された場合、アクワイアラ・ブランドホルダ1から、SCC53およびバス55を介して、価値充填処理が可能であることを示す信号の入力を受けたリーダライタ15のDPU51は、ステップS64において、図15のステップS34と同様の処理を実行する。

【0207】

ステップS65において、図15のステップS35と同様の処理が実行される。

【0208】

ステップS66において、リーダライタ15のDPU51は、バス55、SCC53、パーソナルコンピュータ14、およびインターネット11を介して、アクワイアラ・ブランドホルダ1に処理結果を通知する。

【0209】

ステップS67において、アクワイアラ・ブランドホルダ1のウェブサーバ150は、リーダライタ15から、価値充填処理結果の入力を受け、課金サーバ147に供給する。課金サーバ147は、入力された価値充填処理結果を、入金代行DB148に記録する。

【0210】

ステップS68において、イシュアG/Wサーバ151は、イシュア2-1に、価値充填処理の結果を通知する。なお、価値充填処理結果の通知は、処理が行われる毎に逐次通知するようにしても良いし、例えば1週間や1ヶ月といった、所定の期間毎に行われるようにしても良い。

【0211】

ステップS69およびステップS70において、図15のステップS39およびステップS40と同様の処理が実行される。

【0212】

ステップS61において、正しく認証されなかったと判断された場合、もしくは、ステップS63において、価値充填処理が可能ではないと判断された場合、ステップS71において、アクワイアラ・ブランドホルダ1のウェブサーバ150は、インターネット11を介して、パーソナルコンピュータ14に、エラーメッセージを出力する。

【0213】

ステップS72において、図15のステップS42と同様の処理が実行される。

【0214】

次に、図17乃至図21を参照して、利用者3が、ICカード12に充填された電子マネーを用いて商品を購入したり、各種サービスを受けるための処理と、それらの処理を実行するための鍵の配置の詳細について説明する。

【0215】

まず、図17を用いて、利用者3が、実際の店舗などに赴いて、加盟店舗端末装置18を利用して、ICカード12へ充填された電子マネーを用いて、商品、もしくはサービスの購入を行うことができるようにするための鍵の配置について説明する。

【0216】

図2を用いて上述したように、統括して管理する機構がない店舗4が、単独で、本サービスと提携した場合、アクワイアラ・ブランドホルダ1は、それぞれの店舗4に設置される加盟店舗端末装置18に対して、提携内容に基づいて、対応する鍵を発行して配布する。すなわち、図17の加盟店舗端末装置18-1-1乃至18-1-nは、それぞれの店舗4において提供することができるサービスに対応する鍵を、リーダライタ31-3-1乃至31-3-nにそれぞれ記憶しているので、加盟店舗端末装置18とICカード12との間で認証処理を実行することができる。

【0217】

店舗4は、それぞれの事業に合致したサービスを選択して、本サービスとの提

携を結び、アクワイアラ・ブランドホルダ1より対応する鍵の供給を受けることにより、選択したサービスを利用者3に提供することができる。すなわち、鍵Fもしくは鍵Jが記憶されたICカード12を保有する利用者3は、加盟店端末装置18-1-1を設置している店舗において、鍵Fもしくは鍵Jにより供給可能なサービスを受けることができ、鍵Gが記憶されたICカード12を保有する利用者3は、加盟店端末装置18-1-2を設置している店舗において、鍵Gにより供給可能なサービスを受けることができ、鍵G、鍵Hもしくは鍵Jが記憶されたICカード12を保有する利用者3は、加盟店端末装置18-1-nを設置している店舗において、鍵G、鍵Hもしくは鍵Jにより供給可能なサービスを受けることができる。

【0218】

例えば、チェーン店などの複数の店舗4を有する企業が本サービスと提供した場合、アクワイアラ・ブランドホルダ1は、複数の店舗4を統括するPOSセンタ17に対して鍵を発行して、配布する。加盟店端末装置18-2-1乃至18-2-mは、基本的には、鍵の供給を受けずに、POSセンタ17と接続することにより、ICカード12との認証処理を実行する（加盟店端末装置18-2-1乃至18-2-mが高度なタンバ技術を用いたものであれば、加盟店端末装置18-2-1乃至18-2-mそれぞれに鍵を記憶させて、加盟店端末装置18-2-1乃至18-2-mとICカード12間で認証処理を実行させるようにしても良い）。

【0219】

すなわち、加盟店端末装置18-2-1乃至18-2-mにおいて、鍵Fもしくは鍵Hが記憶されたICカード12を保有する利用者3は、POSセンタ17に保存されている鍵Fもしくは鍵Hにより供給可能なサービスを受けることができるが、リーダライタ31-4-1乃至31-4-mには、鍵Fおよび鍵Hは保存されていない。

【0220】

以下、加盟店舗端末装置18-1-1乃至18-1-nを個々に区別する必要がない場合、単に加盟店舗端末装置18-1と総称し、加盟店舗端末装置18-2

－ 1 乃至 1 8－ 2－ m を個々に区別する必要がない場合、単に加盟店舗端末装置 1 8－ 2 と総称する。

【 0 2 2 1 】

図 1 8 のフローチャートを参照して、 I C カード 1 2 を保有する利用者 3 が、加盟店舗端末装置 1 8－ 1 を利用して、商品もしくはサービスを購入する場合の処理について説明する。

【 0 2 2 2 】

ステップ S 8 1 において、加盟店舗端末装置 1 8－ 1 のリーダライタ 3 1 のアンテナ 4 6 は、所定の電磁波を放射した状態で負荷状態を監視することにより、 I C カード 1 2 を検出し、 D P U 5 1 は、 I C カード 1 2 を検出したことを示す信号を生成し、バス 5 5 および S C C 5 3 を介してコントローラ 3 2 に出力する。

【 0 2 2 3 】

ステップ S 8 2 において、コントローラ 3 2 の制御部 1 0 1 は、ネットワークインターフェース 1 0 7 および内部バス 1 0 2 を介して、リーダライタ 3 1 から送信された信号の入力を受け、利用者 3 に次の操作を促すためのメッセージなどを含むメニュー画面に対応するデータを、内部バス 1 0 2 を介して、表示部 1 0 5 に出力して、メニュー画面を表示させる。

【 0 2 2 4 】

ステップ S 8 3 において、コントローラ 3 2 の制御部 1 0 1 は、内部バス 1 0 2 を介して、入力部 1 0 3 からコマンド（例えば、電子マネー 2 0 0 0 円分の利用を示すコマンド）の入力を受け、内部バス 1 0 2 およびネットワークインターフェース 1 0 7 を介して、リーダライタ 3 1 に出力し、リーダライタ 3 1 は、所定の処理を実行して、入力されたコマンドを I C カード 1 2 に送信する。

【 0 2 2 5 】

ステップ S 8 4 において、図 1 3 のステップ S 4 と同様の処理が実行される。

【 0 2 2 6 】

ステップ S 8 5 において、リーダライタ 3 1 のアンテナ 4 6 は、 I C カード 1 2 から送信された認証情報を受信して、復調回路 4 4 に出力する。復調回路 4 4

において復調されたデータは、SPU52で、BPSK変調などの所定の処理が施され、DPU51に供給される。DPU51は、入力された認証情報を基に、バス55を介して、フラッシュメモリ42から鍵を読み出し、認証処理を実行する。

【0227】

ステップS86において、リーダライタ31のDPU51は、ステップS81において検出されたICカード12は、正しく認証されたか否かを判断する。ステップS86において、ICカード12は正しく認証されなかったと判断された場合、処理は、ステップS94に進む。

【0228】

ステップS86において、ICカード12は正しく認証されたと判断された場合、ステップS87において、リーダライタ31のDPU51は、入力されたコマンドを基に、利用者3が指示したICカード利用処理は可能か否かを、ICカード12から必要な情報を読み出すことなどにより確認する。例えば、2000円分の商品の購入を指示するコマンドが入力された場合、リーダライタ31のDPU51は、ICカード12に、商品の代金に対応する電子マネーが残っているか否かを確認するためのコマンドを生成し、所定の処理を実行して、生成したコマンドをICカード12に送信する。

【0229】

ステップS88において、リーダライタ31のDPU51は、アンテナ46を介して、ICカード12から入力される問い合わせに対するレスポンス信号などを基に、コマンド処理は可能か否かを判断する。ステップS88において、コマンド処理ができないと判断された場合、処理は、ステップS94に進む。

【0230】

ステップS88において、コマンド処理が可能であると判断された場合、ステップS89において、リーダライタ31のDPU51は、ICカード12に対して価値充填処理を実行させる（ICカード12の対象となるファイルに記録されている電子マネーの値から、所定の値を減算させる）ためのコマンドを生成して、バス55を介してSPU52に出力する。そして、SPU52および変調回路

4 3 において所定の処理が施されて、コマンドに対応する変調波が生成され、アンテナ 4 6 を介して、電磁波として I C カード 1 2 に出力される。

【 0 2 3 1 】

ステップ S 9 0 において、I C カード 1 2 のアンテナ 7 3 は、リーダライタ 3 1 のアンテナ 4 6 より、変調波を受信する。そして、インターフェース部 8 1、B P S K 復調部 8 2、および演算部 8 4 において所定の処理が実行され、EEPROM 8 6 に記録された電子マネーの減算に対応するコマンド処理が実行され、結果が保存される。

【 0 2 3 2 】

ステップ S 9 1 において、コントローラ 3 2 の制御部 1 0 1 は、コマンド処理結果を、内部バス 1 0 2 およびネットワークインターフェース 1 0 7 を介して、アクワイアラ・ブランドホルダ 1 に通知する。なお、コマンド処理結果の通知は、処理が行われる毎に逐次通知するようにしても良いし、例えば 1 週間や 1 ヶ月といった、所定の期間毎に行われるようにしても良い。

【 0 2 3 3 】

ステップ S 9 2 において、コントローラ 3 2 の制御部 1 0 1 は、コマンド処理結果のログを I C カード 1 2 に記録させるための制御信号を生成して、内部バス 1 0 2 およびネットワークインターフェース 1 0 7 を介して、リーダライタ 3 1 に送信し、リーダライタ 3 1 の D P U 5 1 は、S C C 5 3 およびバス 5 5 を介して入力された信号を基に、I C カード 1 2 に送信するコマンドを、バス 5 5 を介して S P U 5 2 に出力する。S P U 5 2 および変調回路 4 3 で所定の処理が施されて、コマンドに対応する変調波が生成され、アンテナ 4 6 を介して、電磁波として I C カード 1 2 に出力される。

【 0 2 3 4 】

ステップ S 9 3 において、I C カード 1 2 のアンテナ 7 3 は、リーダライタ 3 1 より、変調波を受信する。そして、インターフェース部 8 1、B P S K 復調部 8 2、および演算部 8 4 において所定の処理が実行され、EEPROM 8 6 にコマンド処理のログが書き込まれ、保存される。

【 0 2 3 5 】

ステップ S 8 6 において、I C カード 1 2 が正しく認証されなかったと判断された場合、もしくは、ステップ S 8 8 において、コマンド処理が可能ではないと判断された場合、ステップ S 9 4 において、コントローラ 3 2 の制御部 1 0 1 は、内部バス 1 0 2 を介して、表示部 1 0 5 にエラーメッセージを出力して、表示させる。

【 0 2 3 6 】

次に、図 1 9 のフローチャートを参照して、I C カード 1 2 を保有する利用者 3 が、加盟店舗端末装置 1 8 - 2 を利用して、商品、もしくはサービスを購入する場合の処理について説明する。

【 0 2 3 7 】

ステップ S 1 0 1 乃至ステップ S 1 0 4 において、図 1 8 のステップ S 8 1 乃至ステップ S 8 4 と同様の処理が実行される。

【 0 2 3 8 】

ステップ S 1 0 5 において、リーダライタ 3 1 のアンテナ 4 6 は、I C カード 1 2 から送信された認証情報を受信して、復調回路 4 4 に出力する。復調回路 4 4 において復調されたデータは、S P U 5 2 で、B P S K 変調などの所定の処理が施され、D P U 5 1 に供給される。D P U 5 1 は、認証処理を依頼するための信号を生成して、バス 5 5 および S C C 5 3 を介して、入力された認証情報とともに、コントローラ 3 2 へ出力する。コントローラ 3 2 の制御部 1 0 1 は、ネットワークインターフェース 1 0 7 および内部バス 1 0 2 を介して、認証処理を依頼するための信号、および認証情報の入力を受け、内部バス 1 0 2 およびネットワークインターフェース 1 0 7 を介して、利用者 3 の指令を示すコマンドとともに、対応する P O S センタ 1 7 に送信する。

【 0 2 3 9 】

ステップ S 1 0 6 において、P O S センタ 1 7 の C P U 1 2 1 は、ネットワークインターフェース 1 2 5、入出力インターフェース 1 2 2 および内部バス 1 2 3 を介して入力された認証処理依頼および認証情報に基づいて、アクワイアラ・ブランドホルダ 1 から供給され、R A M 1 2 7 もしくは H D D 1 2 9 に保存している鍵を読み出して認証処理を行う。

【0240】

ステップS107において、POSセンタ17のCPU121は、ステップS106で実行された認証処理において、ステップS101において検出されたICカード12は、正しく認証されたか否かを判断する。ステップS107において、ICカード12は正しく認証されなかったと判断された場合、処理は、ステップS117に進む。

【0241】

ステップS107において、ICカード12は正しく認証されたと判断された場合、ステップS108において、POSセンタ17のCPU121は、内部バス123、入出力インターフェース122、およびネットワークインターフェース125を介して、正しく認証されたことを、加盟店端末装置18-2に通知する。

【0242】

ステップS109乃至ステップS112において、図18のステップS87乃至ステップS90と、同様の処理が実行される。

【0243】

ステップS113において、コントローラ32の制御部101は、ネットワークインターフェース107および内部バス102を介して、POSセンタ17に処理結果を通知する。

【0244】

ステップS114において、POSセンタ17のCPU121は、内部バス123、入出力インターフェース122、およびネットワークインターフェース125を介して、コマンド処理結果を、アクワイアラ・ブランドホルダ1に通知する。なお、コマンド処理結果の通知は、処理が行われる毎に逐次通知するようにしても良いし、例えば1週間や1ヶ月といった、所定の期間毎に行われるようにしても良い。

【0245】

ステップS115およびステップS116において、図18のステップS92およびステップS93と同様の処理が実行される。

【0246】

ステップS107において、正しく認証されなかったと判断された場合、もしくは、ステップS110において、コマンド処理が可能ではないと判断された場合、ステップS117において、POSセンタ17のCPU121は、内部バス123、入出力インターフェース122、およびネットワークインターフェース125を介して、加盟店端末装置18-2に、エラーメッセージを出力する。

【0247】

ステップS108において、図18のステップS94と同様の処理が実行される。

【0248】

なお、図17および図19においては、ICカード12を保有する利用者3が、加盟店端末装置18-2を利用する場合の処理について説明したが、MMKセンタ19に統括管理されているMMK20を利用する場合においても、POSセンタ17に統括管理されている加盟店端末装置18-2における処理と、基本的に同様の処理が実行される。

【0249】

次に、図20を用いて、利用者3が、実際の店舗などに赴くことなく、ICカード12に充填された電子マネーを用いて、インターネット11に公開されているサイバー店舗16において商品を購入したり、各種サービスを受けるための処理と、それらの処理を実行するための鍵の配置の詳細について説明する。

【0250】

インターネット11と接続している複数のサイバー店舗16-1乃至16-mは、アクワイアラ・ブランドホルダ1との提携内容に基づいて、インターネット11に接続することが可能なパーソナルコンピュータ14-1乃至14-n、および、パーソナルコンピュータ14-1乃至14-nに接続されたリーダライタ15-1乃至15-nを利用する、ICカード12を保有する利用者3に対して、各種サービスを提供することが可能なようになされている。

【0251】

サイバー店舗16-1乃至16-mは、例えば、インターネット11を介して

、利用者3が保有するパーソナルコンピュータ14に、購入希望画面などを出力したり、パーソナルコンピュータ14から、ICカード12の認証情報や、利用者3が購入を希望する商品についての情報の入力を受けるためのウェブサーバ193-1乃至193-m、商品の在庫や売上に関する情報を記録するための在庫／売上管理DB192-1乃至192-mを管理し、サービス提供に関する処理を実行する売上管理サーバ191-1乃至191-mを備えている。

【0252】

以下、売上管理サーバ191-1乃至191-mを個々に区別する必要がない場合、単に、売上管理サーバ191と総称し、在庫／売上管理DB192-1乃至192-mを個々に区別する必要がない場合、単に、在庫／売上管理DB192と総称し、ウェブサーバ193-1乃至193-mを個々に区別する必要がない場合、単に、ウェブサーバ193と総称する。なお、売上管理サーバ191およびウェブサーバ193の構成は、図8を用いて説明したパーソナルコンピュータ14と基本的に同様であるので、その説明は省略する。

【0253】

アクワイアラ・ブランドホルダ1は、サイバー店舗16-1乃至16-mそれぞれとの提携内容に基づいて、鍵K、鍵L、もしくは鍵Mを発行した場合においても、発行した鍵をサイバー店舗16-1乃至16-mに配布しない。アクワイアラ・ブランドホルダ1のセキュリティサーバ145は、鍵管理DB146に、サイバー店舗16-1乃至16-mそれぞれに、いずれの鍵を発行したかを登録しているので、サイバー店舗16-1乃至16-mのいずれかから、認証処理を依頼された場合、鍵管理DB146を参照して、認証処理を実行し、認証処理結果を、対応するサイバー店舗16-1乃至16-mのいずれかに、インターネット11を介して出力する。

【0254】

すなわち、サイバー店舗16-1乃至16-mは、いずれの鍵も記録しない。サイバー店舗16-1乃至16-mは、インターネット11を介して、パーソナルコンピュータ14から、リーダライタ15で読み込まれたICカード12の認証情報の入力を受けた場合、その認証情報を、インターネット11を介して、ア

クワイアラ・ブランドホルダ 1 に出力し、認証処理を依頼し、インターネット 1 1 を介して、アクワイアラ・ブランドホルダ 1 から、認証処理結果の入力を受ける。

【 0 2 5 5 】

図 2 1 のフローチャートを参照して、IC カード 1 2 を保有する利用者 3 が、パーソナルコンピュータ 1 4 を用いて、インターネット 1 1 を介して、サイバー店舗 1 6 にアクセスし、商品、もしくはサービスを購入する場合の処理について説明する。

【 0 2 5 6 】

ステップ S 1 2 1 において、図 1 5 のステップ S 2 1 と同様の処理が実行される。

【 0 2 5 7 】

ステップ S 1 2 2 において、パーソナルコンピュータ 1 4 の CPU 1 2 1 は、内部バス 1 2 3、入出力インターフェース 1 2 2、ネットワークインターフェース 1 2 5、およびインターネット 1 1 を介して、サイバー店舗 1 6 に接続する。

【 0 2 5 8 】

ステップ S 1 2 3 において、サイバー店舗 1 6 のウェブサーバ 1 9 3 は、インターネット 1 1 を介して、パーソナルコンピュータ 1 4 に、購入希望画面に対応するデータを出力する。

【 0 2 5 9 】

ステップ S 1 2 4 において、パーソナルコンピュータ 1 4 の CPU 1 2 1 は、ネットワークインターフェース 1 2 5、入出力インターフェース 1 2 2、および内部バス 1 2 3 を介して入力された、購入希望画面に対応するデータを、内部バス 1 2 3 および入出力インターフェース 1 2 2 を介して、表示部 1 2 8 に出力して、入力希望画面を表示させる。入力希望画面には、リーダライタ 1 5 と IC カード 1 2 が通信可能な状態となるように、IC カード 1 2 を所定の読み取り位置に設置することを促すためのメッセージ、および、操作の入力を促すメニューなどが表示される。ここでは、IC カード 1 2 を用いた商品の購入処理が利用者 3 によって選択され、入力部 1 2 4 を用いて指示されたものとする。

【0260】

ステップS125乃至ステップS128において、図15のステップS25乃至ステップS28と同様の処理が実行される。

【0261】

ステップS129において、パーソナルコンピュータ14のCPU121は、ネットワークインターフェース125、入出力インターフェース122、および内部バス123を介して、認証情報の入力を受け、利用者3が実行した操作に対応するコマンド（ここでは、ICカード12を用いた商品購入処理を実行するためのコマンド）とともに、サイバー店舗16に送信する。

【0262】

ステップS130において、サイバー店舗16のウェブサーバ193は、認証情報の入力を受け、アクワイアラ・ブランドホルダ1に対して認証処理を依頼する信号を生成し、入力された認証情報とともに、アクワイアラ・ブランドホルダ1に出力する。アクワイアラ・ブランドホルダ1のウェブサーバ150は、入力された情報を、セキュリティサーバ145に出力する。セキュリティサーバ145は、入力された認証処理依頼および認証情報に基づいて、鍵管理DB146に保存している、対応するサイバー店舗16に発行した鍵との認証処理を行い、認証処理結果を、インターネット11を介して、サイバー店舗16に出力する。

【0263】

サイバー店舗16の売上管理サーバ191は、ステップS131において、アクワイアラ・ブランドホルダ1から、インターネット11およびウェブサーバ193を介して、認証結果の入力を受け、ステップS132において、ステップS125において検出されたICカード12は、正しく認証されたか否かを判断する。ステップS132において、ICカード12は正しく認証されなかったと判断された場合、処理は、ステップS144に進む。

【0264】

ステップS133において、サイバー店舗16の売上管理サーバ191は、正しく認証されたことを、ウェブサーバ193、およびインターネット11を介して、パーソナルコンピュータ14に通知する。

【0265】

ステップS134において、パーソナルコンピュータ14のCPU121は、入力された認証結果を、内部バス123、入出力インターフェース122、および、ネットワークインターフェース125を介して、リーダライタ15に出力する。

【0266】

ステップS135において、リーダライタのDPU51は、入力された認証結果を基に、利用者3が指示したICカード利用処理（例えば、2000円分の商品の購入）は可能か否か（ICカード12に、商品の代金に対応する電子マネーが残っているか否か）を、ICカード12から必要な情報を読み出し、パーソナルコンピュータ14、インターネット11を介して、アクワイアラ・ブランドホルダ1に、売上承認要求を送信し、そのレスポンスを受けることなどにより確認する。

【0267】

ステップS136において、リーダライタ15のDPU51は、アンテナ46を介して、ICカード12から入力される問い合わせに対するレスポンス信号を、バス55およびSCC53を介して、パーソナルコンピュータ14に出力し、パーソナルコンピュータ14のCPUは、リーダライタ15から入力されたレスポンス、および、インターネット11を介して、アクワイアラ・ブランドホルダ1から入力された売上承認要求に対するレスポンスを基に、コマンド処理は可能か否かを判断する。ステップS136において、コマンド処理ができないと判断された場合、処理は、ステップS144に進む。

【0268】

ステップS136において、コマンド処理が可能であると判断された場合、ステップS137において、リーダライタ15のDPU51は、ICカード12に対して価値充填処理を実行させる（ICカード12の対象となるファイルに記録されている電子マネーの値から、所定の値を減算する）ためのコマンドを生成して、バス55を介してSPU52に出力する。SPU52および変調回路43において所定の処理が施されて、コマンドに対応する変調波が生成され、アンテナ

46を介して、電磁波としてICカード12に送信される。

【0269】

ステップS138において、図18のステップS90と同様の処理が実行される。

【0270】

ステップS139において、リーダライタのDPU51は、バス55、SCC53、パーソナルコンピュータ14、およびインターネット11を介して、コマンド処理結果を、サイバー店舗16に通知する。

【0271】

サイバー店舗16の売上管理サーバ191は、ステップS140において、在庫／売上管理DB192を更新し、ステップS141において、ウェブサーバ193、およびインターネット11を介して、アクワイアラ・ブランドホルダ1に処理結果を通知する。なお、コマンド処理結果の通知は、処理が行われる毎に逐次通知するようにしても良いし、例えば1週間や1ヶ月といった、所定の期間毎に行われるようにしても良い。

【0272】

ステップS142およびステップS143において、図15のステップS39およびステップS40と同様の処理が実行される。

【0273】

ステップS132において、正しく認証されなかったと判断された場合、もしくは、ステップS136において、コマンド処理が可能ではないと判断された場合、ステップS144において、サイバー店舗16の売上管理サーバ191は、ウェブサーバ193およびインターネット11を介して、パーソナルコンピュータ14に、エラーメッセージを出力する。

【0274】

ステップS145において、図15のステップS42と同様の処理が実行される。

【0275】

以上説明した処理においては、非接触ICカードを用いた情報の授受が行われ

る場合について説明したが、利用者3が保有する、電子マネーなどの情報を記録し、各種処理を行うためのハードウェアは、例えば、接触型ICカード、携帯電話、PDA、パーソナルコンピュータ、時計などの、様々な情報処理機器が用いられるようにしても良い。

【0276】

上述した一連の処理は、ソフトウェアにより実行することもできる。そのソフトウェアは、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、記録媒体からインストールされる。

【0277】

この記録媒体は、図4、図7、あるいは図8に示すように、コンピュータとは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク65、111、もしくは131（フロッピーディスクを含む）、光ディスク66、112、もしくは132（CD-ROM（Compact Disk-Read Only Memory）、DVD（Digital Versatile Disk）を含む）、光磁気ディスク67、113、もしくは133（MD（Mini-Disk）を含む）、あるいは、半導体メモリ68、114、もしくは134などよりなるパッケージメディアなどにより構成される。

【0278】

また、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【0279】

なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【0280】

【発明の効果】

本発明の情報処理装置、情報処理方法、および記録媒体に記録されているプログラムによれば、電子マネー情報、および電子マネーサービスに関する認証処理に用いられる認証情報が記録される第1の情報処理装置を発行する第2の事業者が管理する第2の情報処理装置と情報を授受し、電子マネーを利用したサービスを提供する第3の事業者が管理する第3の情報処理装置と情報を授受し、電子マネーサービスに関する認証処理に用いられる認証情報を記録し、第2の事業者に関する情報、および第1の事業者と第2の事業者との提携内容に関する情報を記録し、第3の事業者に関する情報、および第1の事業者と第3の事業者との提携内容に関する情報を記録し、第1の事業者と第2の事業者との提携内容に関する情報に基づいて、認証情報を出力し、第1の事業者と第3の事業者との提携内容に関する情報に基づいて、認証情報を出力するようにしたので、電子マネー事業において、1つのブランドを管理する事業体が管理する情報処理装置において、イシューおよび加盟店に対する暗号鍵の配布、およびシステムの運営・管理を一元化し、事業体として必要なコストを低減することができる。

【 0 2 8 1 】

本発明の電子マネーサービス提供システムによれば、第1の情報処理装置で、第2の事業者が管理する第3の情報処理装置と情報を授受し、第3の事業者が管理する第4の情報処理装置と情報を授受し、電子マネーサービスに関する認証処理に用いられる認証情報を記録し、第2の事業者に関する情報、および第1の事業者と第2の事業者との提携内容に関する情報を記録し、第3の事業者に関する情報、および第1の事業者と第3の事業者との提携内容に関する情報を記録し、第1の事業者と第2の事業者との提携内容に関する情報に基づいて、認証情報を出力し、第1の事業者と第3の事業者との提携内容に関する情報に基づいて、認証情報を出力し、第2の情報処理装置で、認証情報を記録し、電子マネー情報を記録し、第3の情報処理装置で、第1の情報処理装置と情報を授受し、入力された認証情報を記録し、第2の情報処理装置の発行に関する情報を記録し、記録された認証情報に基づいて、第2の情報処理装置との認証処理を実行し、第4の情報処理装置で、第1の情報処理装置と情報を授受し、入力された認証情報を記録し、記録された認証情報に基づいて、第2の情報処理装置との認証処理を実行す

るようにしたので、電子マネー事業において、1つのブランドに対して、多くのイシューおよび加盟店が参画することができ、イシューおよび加盟店に対する暗号鍵の配布、およびシステムの運営・管理に必要なコストを低減することができる。

【図面の簡単な説明】

【図1】

本発明を適応した電子マネーサービス提供システムの構成を説明するための図である。

【図2】

電子マネーサービス提供システムにおけるネットワーク接続の構成、および、アクワイアラ・ブランドホルダによる鍵の発行について説明するための図である。

【図3】

ICカード、リーダライタ、およびコントローラについて説明するための図である。

【図4】

図3のリーダライタの構成を示すブロック図である。

【図5】

図3のICカードの構成を示すブロック図である。

【図6】

図5のEEPROMの論理フォーマットについて説明するための図である。

【図7】

図3のコントローラの構成を示すブロック図である。

【図8】

図2のパーソナルコンピュータの構成を示すブロック図である。

【図9】

アクワイアラ・ブランドホルダの構成を示すブロック図である。

【図10】

イシューの構成を示すブロック図である。

【図 1 1】

イシューアの構成を示すブロック図である。

【図 1 2】

入金端末装置もしくはMMKにおいて電子マネーの充填処理を実行するための鍵の配置について説明するための図である。

【図 1 3】

入金端末装置もしくはMMKにおける電子マネーの充填処理について説明するためのフローチャートである。

【図 1 4】

インターネットを介した電子マネーの充填処理を実行するための鍵の配置について説明するための図である。

【図 1 5】

インターネットを介した電子マネーの充填処理について説明するためのフローチャートである。

【図 1 6】

インターネットを介した電子マネーの充填処理をアクワイアラ・ブランドホルダが代行する場合の処理について説明するためのフローチャートである。

【図 1 7】

店舗において、ICカードを用いた商品、もしくはサービスの購入処理を可能とするための鍵の配置について説明するための図である。

【図 1 8】

店舗における、ICカードを用いた商品、もしくはサービスの購入処理について説明するためのフローチャートである。

【図 1 9】

店舗における、ICカードを用いた商品、もしくはサービスの購入処理について説明するためのフローチャートである。

【図 2 0】

サイバー店舗において、ICカードを用いた商品、もしくはサービスの購入処理を可能とするための鍵の配置について説明するための図である。

【図 21】

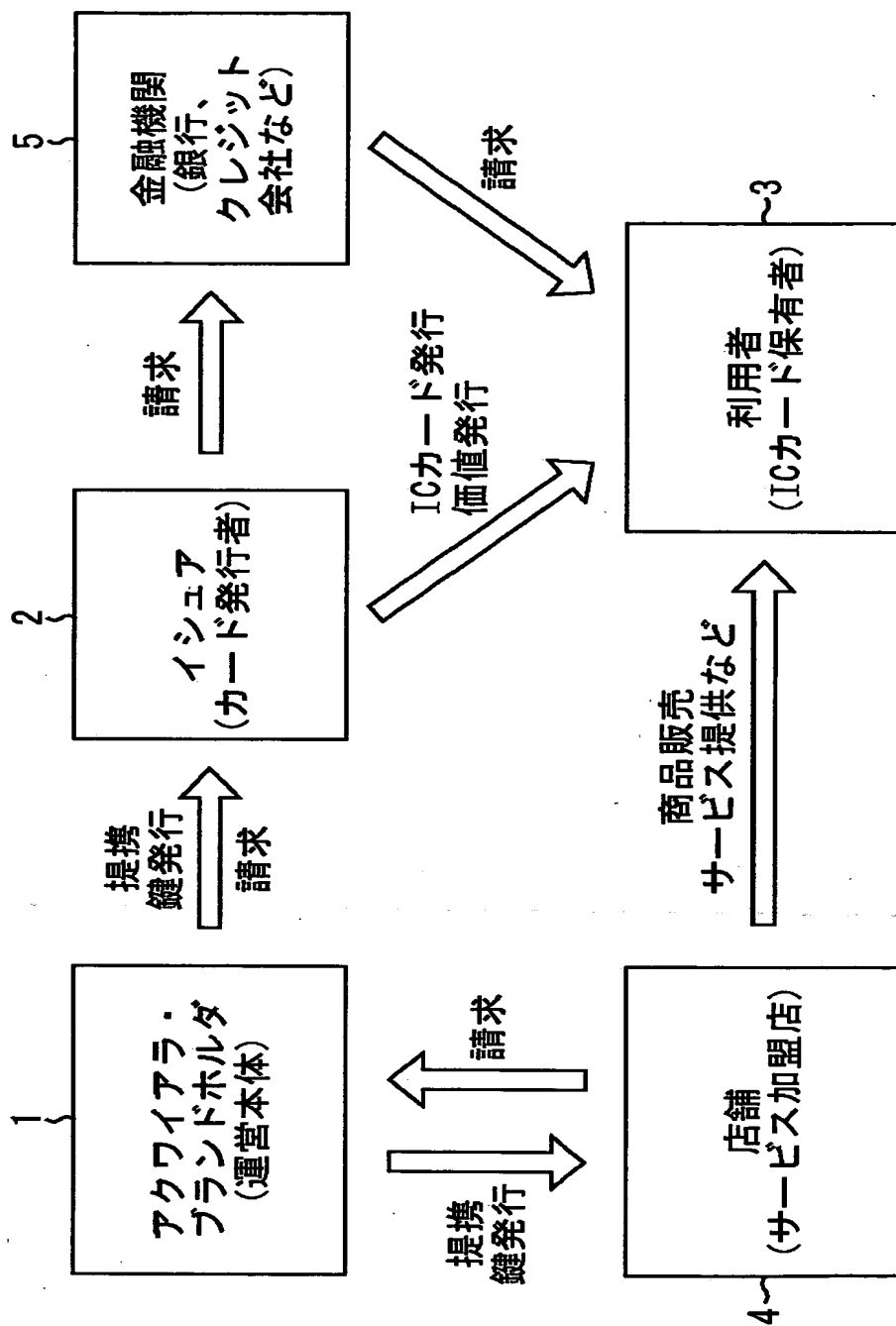
サイバー店舗における、ICカードを用いた商品、もしくはサービスの購入処理について説明するためのフローチャートである。

【符号の説明】

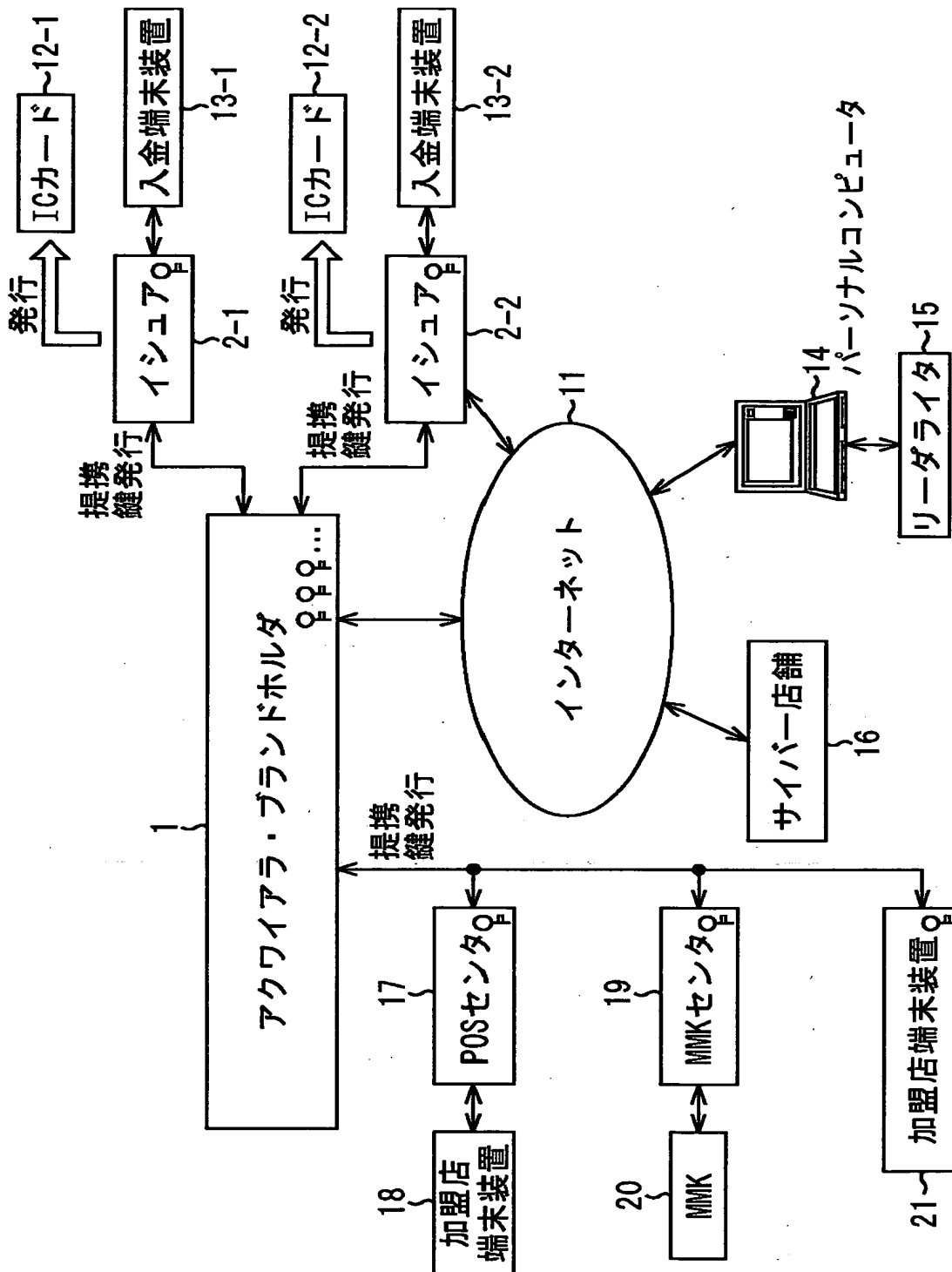
1 アクワイアラ・ブランドホルダ、 2 イシュア、 4 店舗、 11 インターネット、 12 ICカード、 13 入金端末装置、 14 パーソナルコンピュータ、 15 リーダライタ、 16 サイバー店舗、 17 POSセンタ、 18 加盟店端末装置、 19 MMKセンタ、 20 MMK、 21 加盟店端末装置、 31 リーダライタ、 32 コントローラ、 141 店舗管理サーバ、 142 店舗管理DB、 143 顧客サーバ、 144 顧客DB、 145 セキュリティサーバ 146 鍵管理DB、 147 課金サーバ、 148 入金代行DB、 149 店舗G/Wサーバ、 150 ウェブサーバ、 151 イシュアG/Wサーバ

【書類名】図面

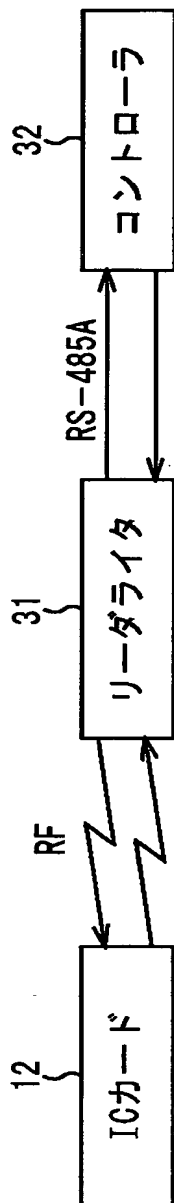
【図 1】



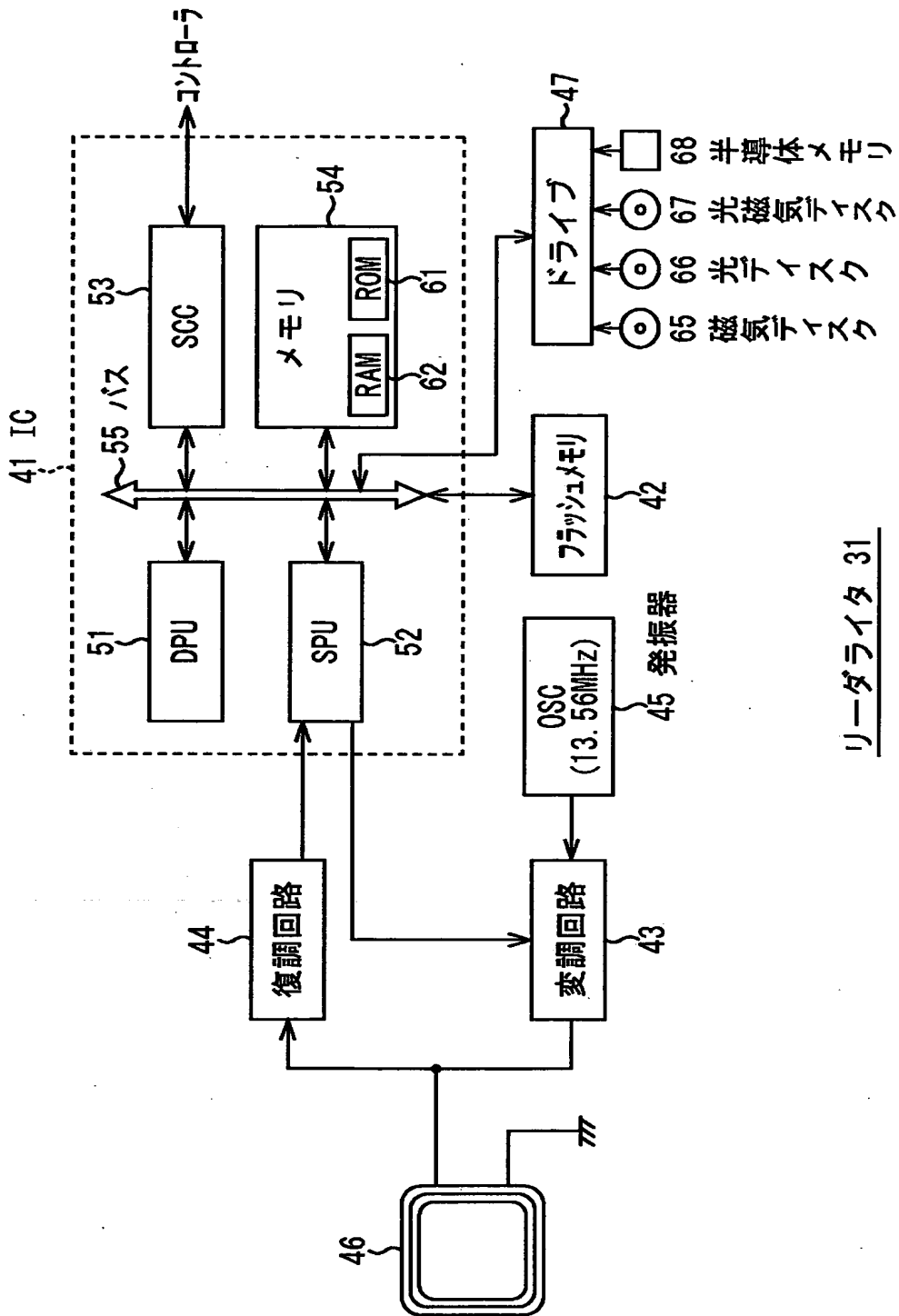
【図2】



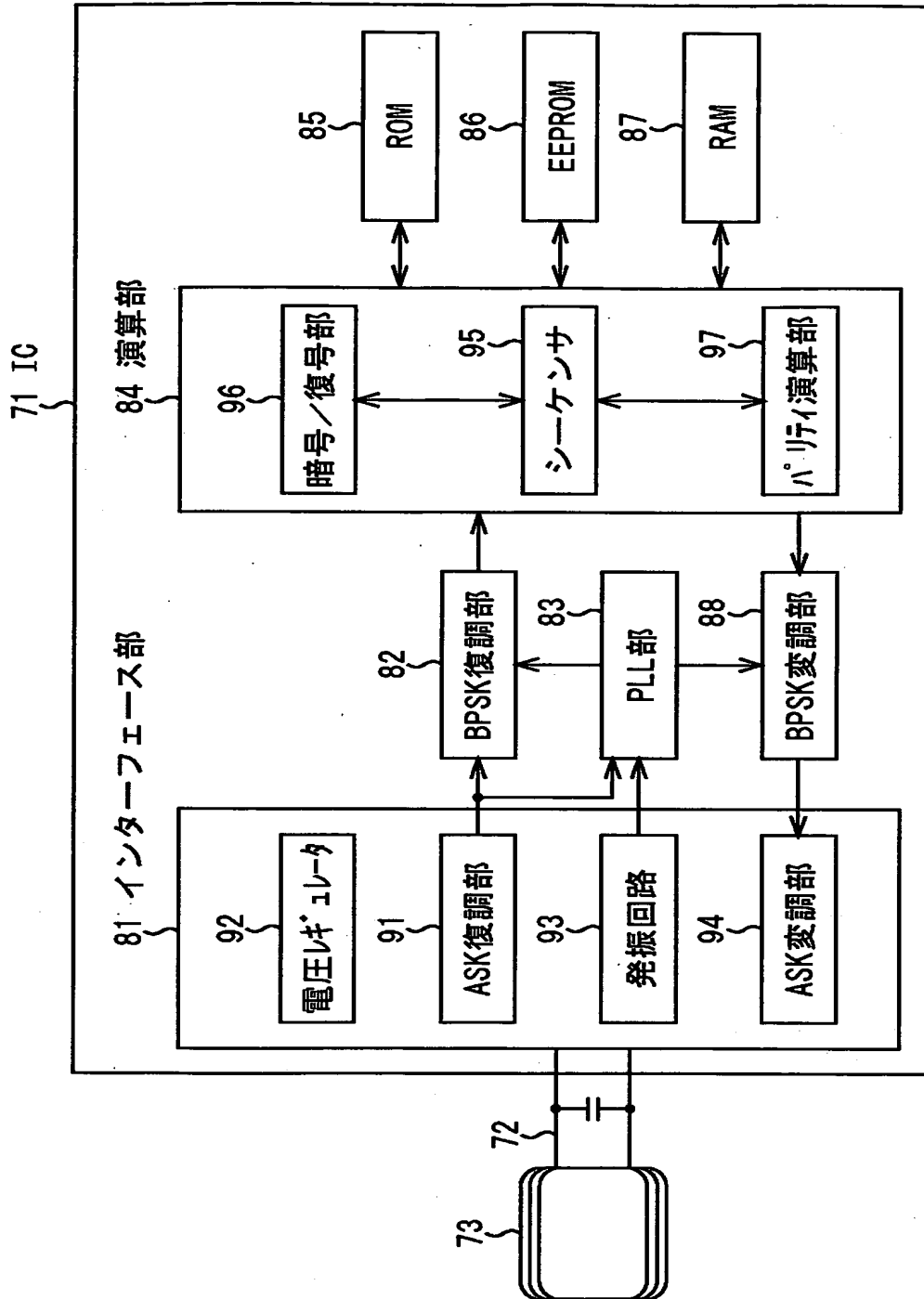
【図3】



【図4】

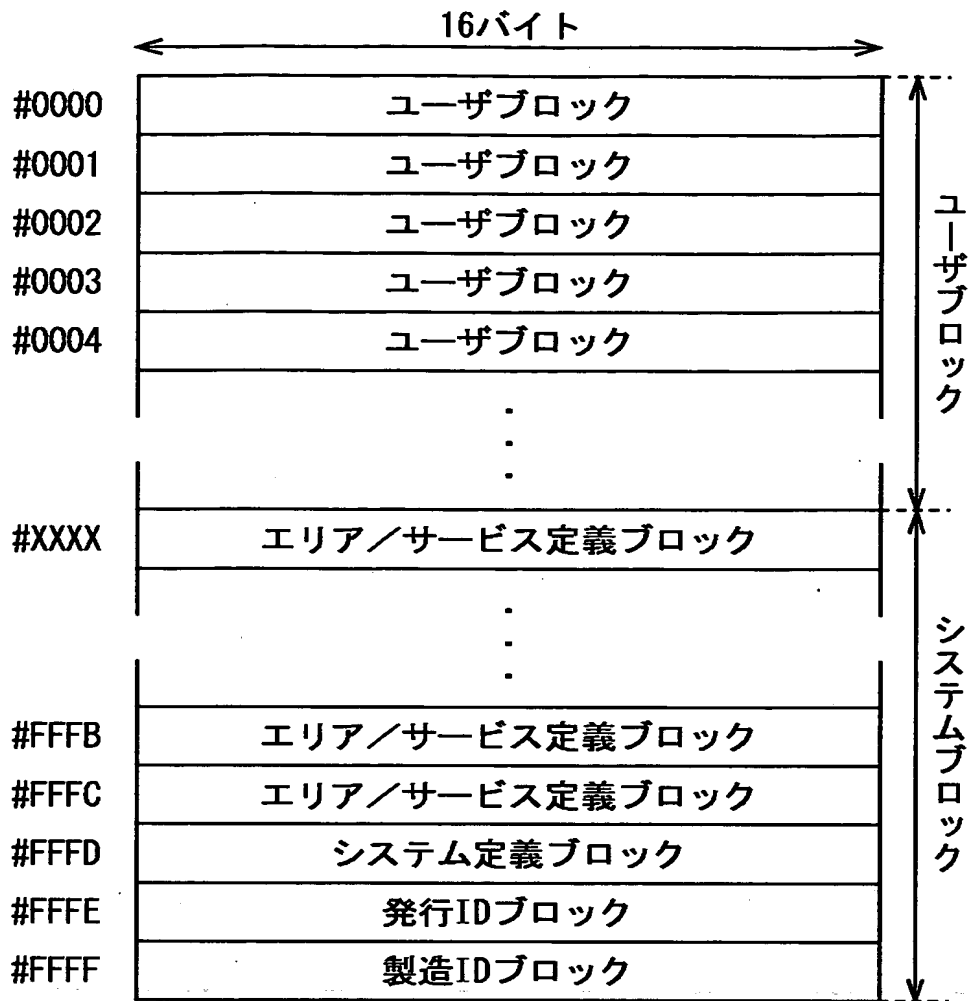


【図 5】



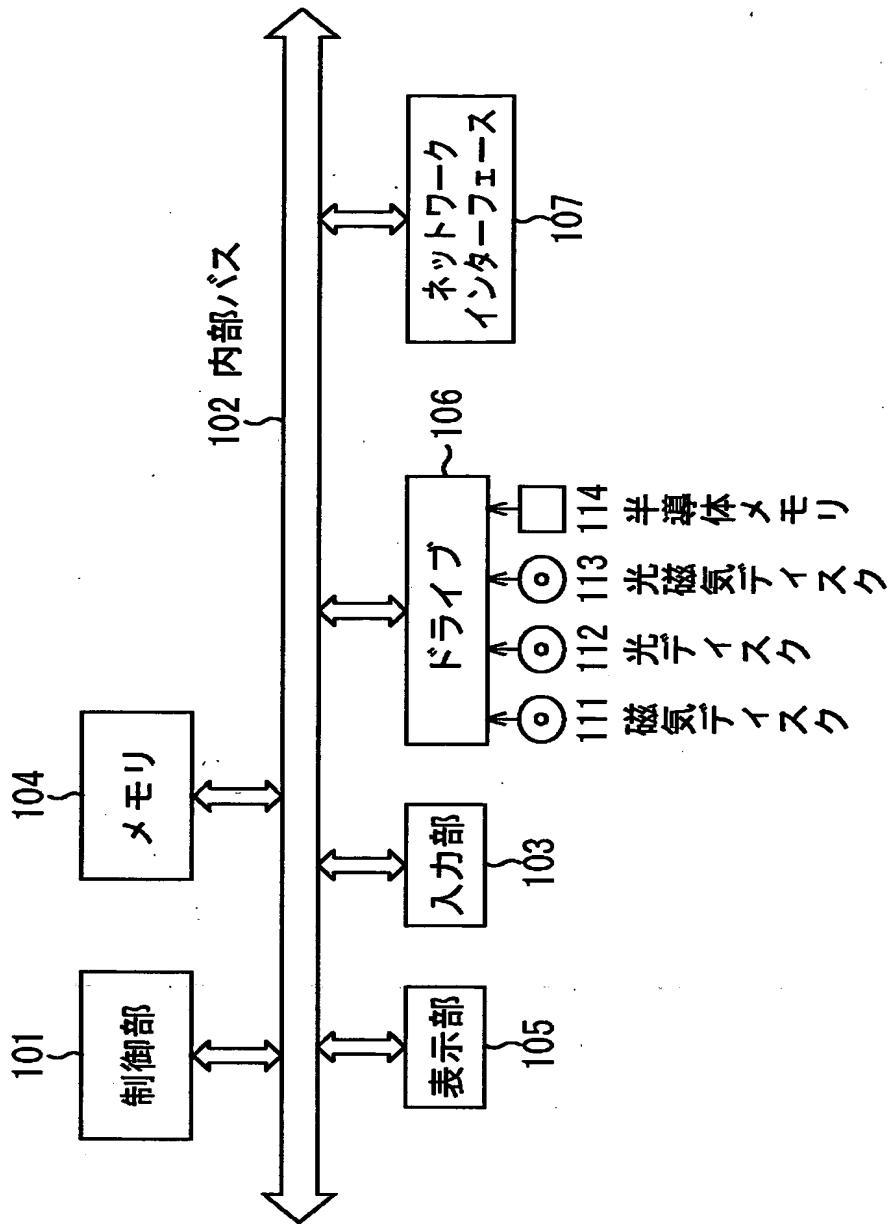
ICカード 12

【図 6】



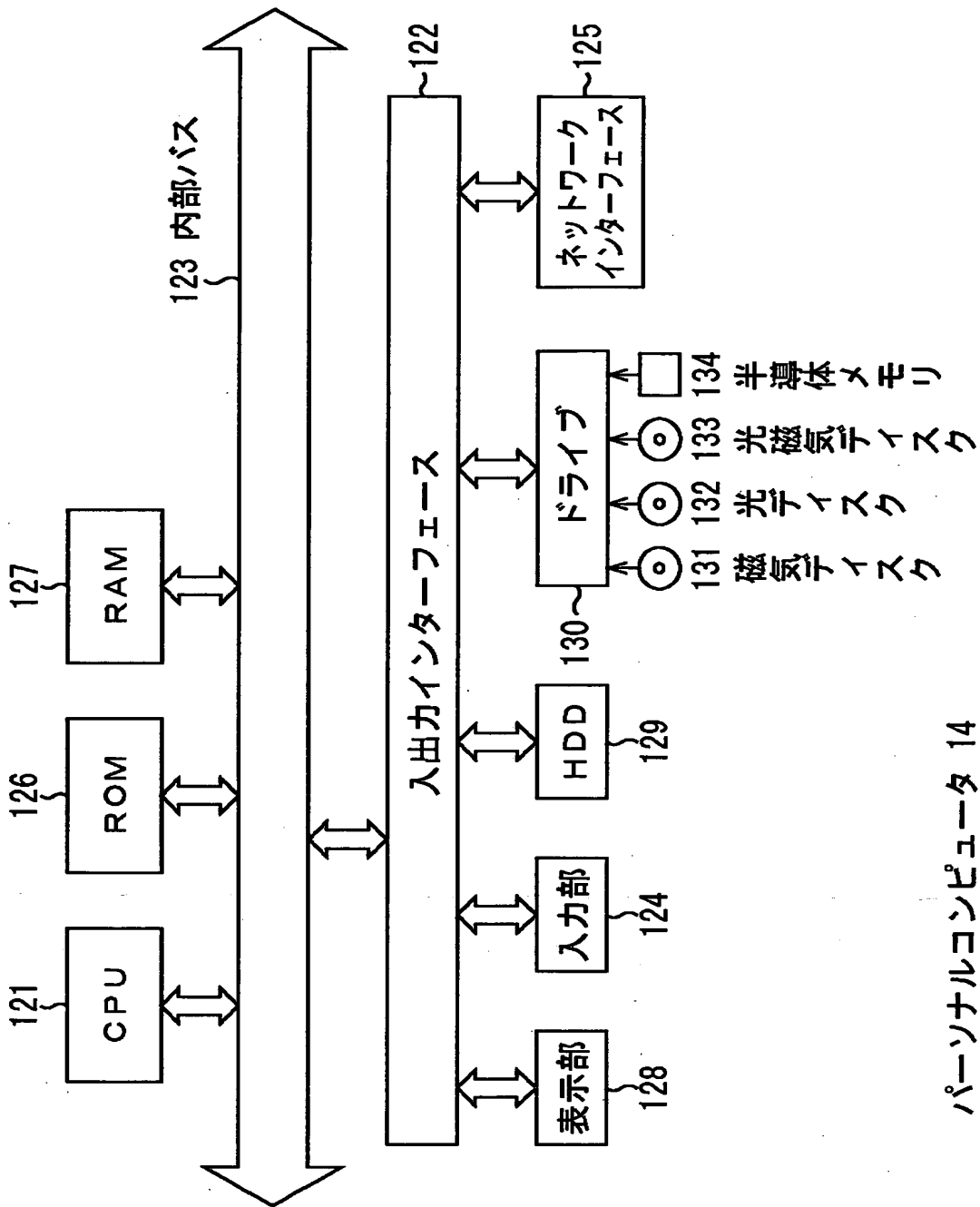
EEPROM86の論理フォーマット

【図 7】



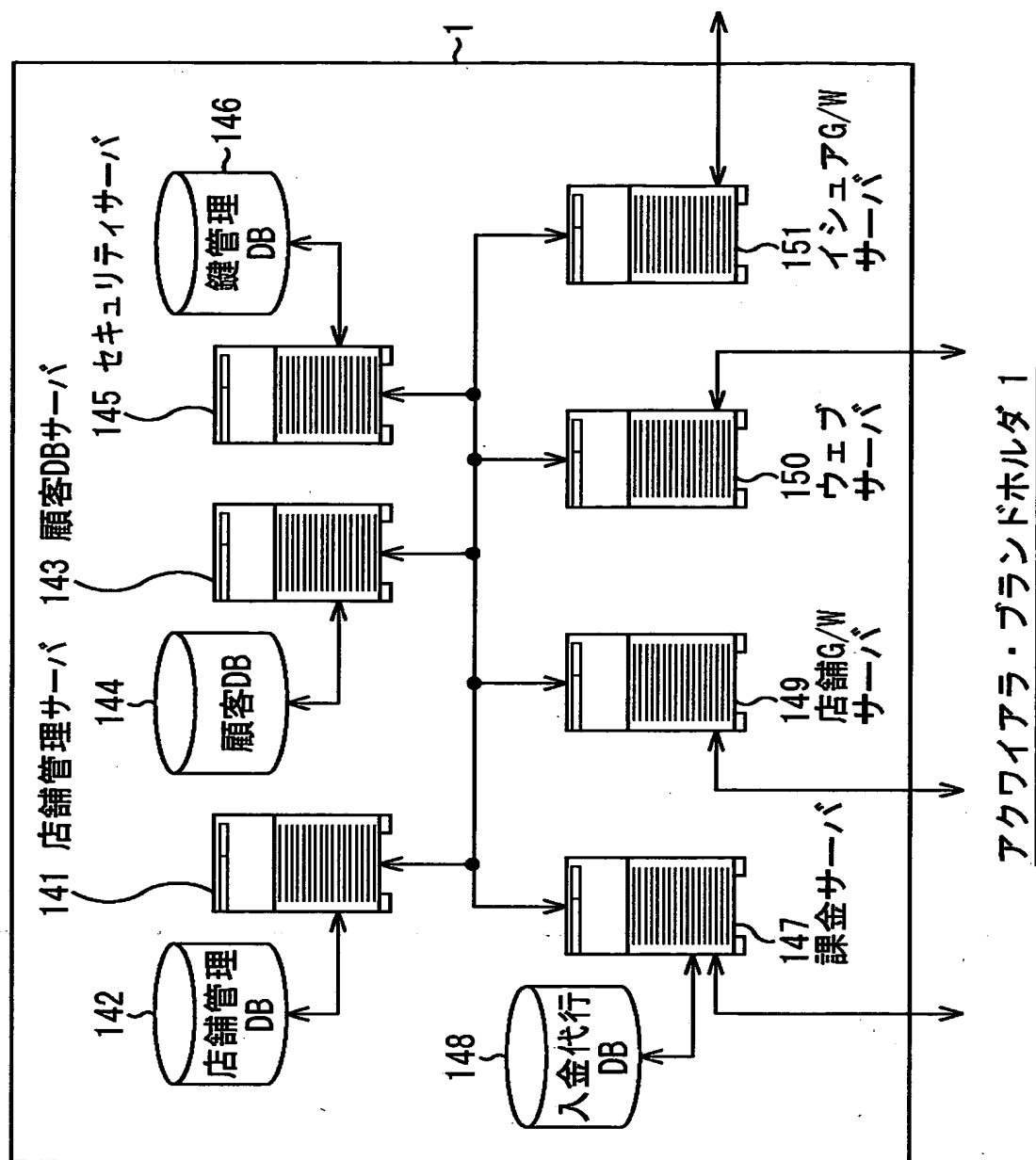
コントローラ 32

【図 8】

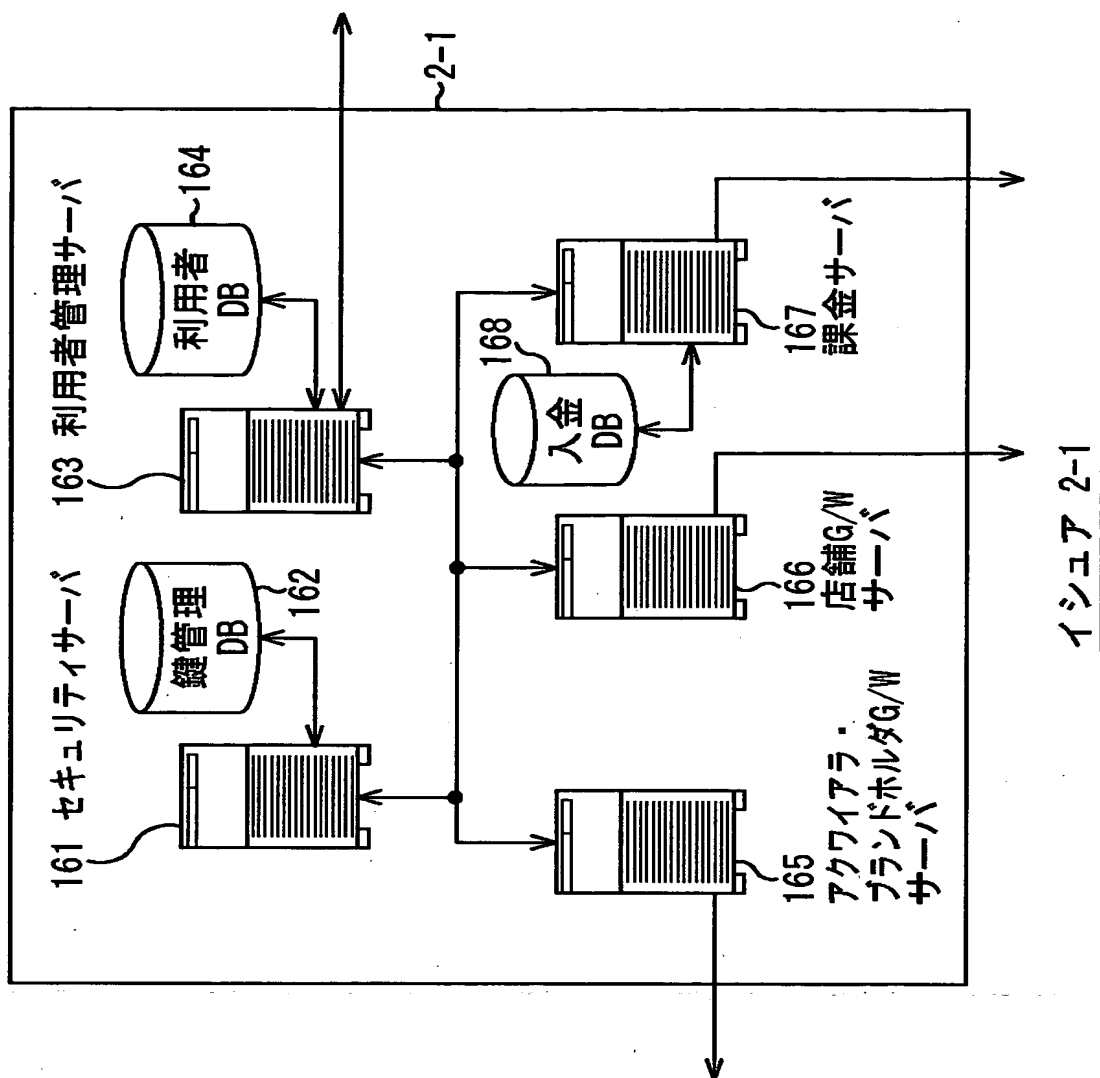


パーソナルコンピュータ 14

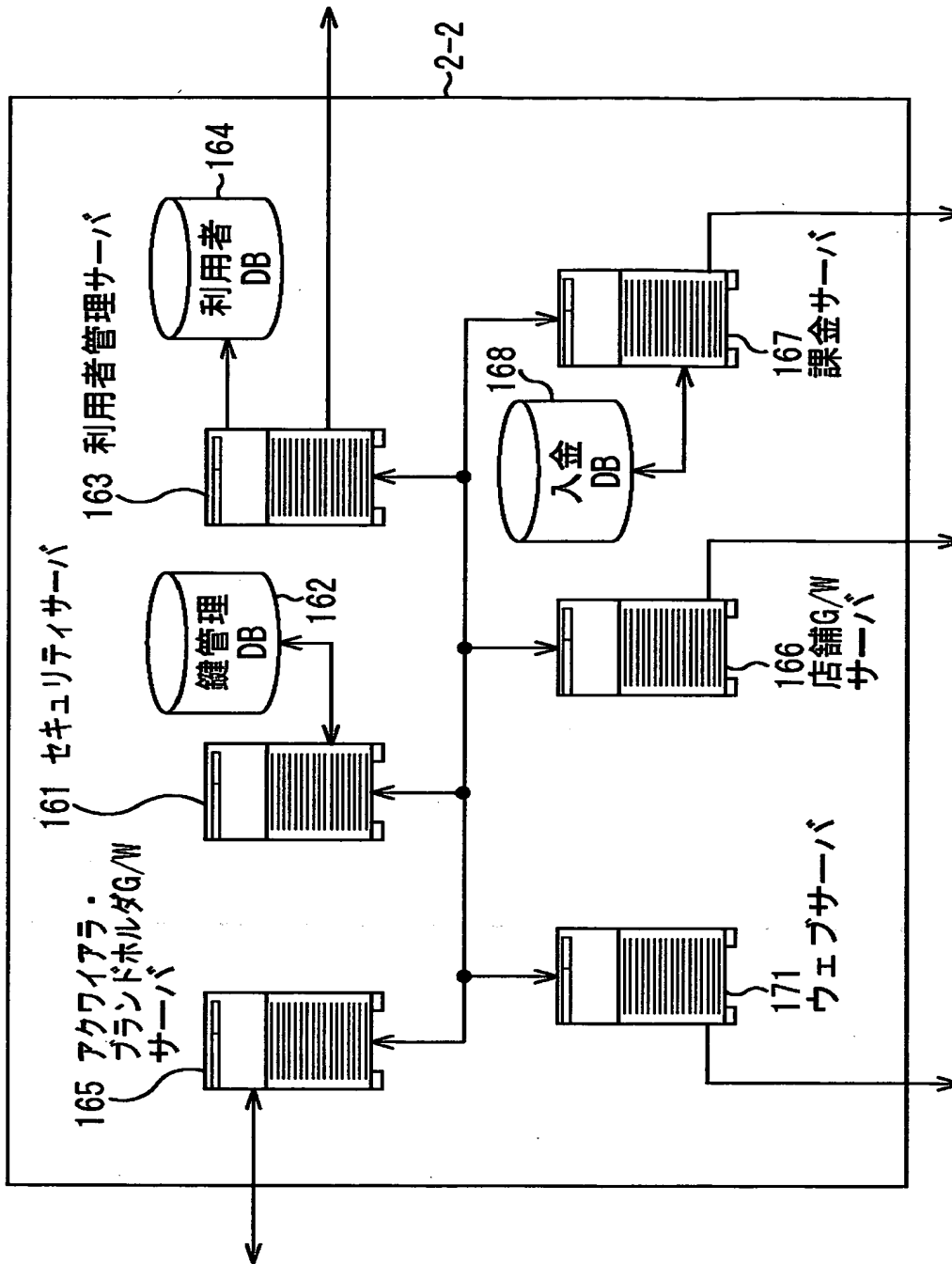
【図9】



【図 10】

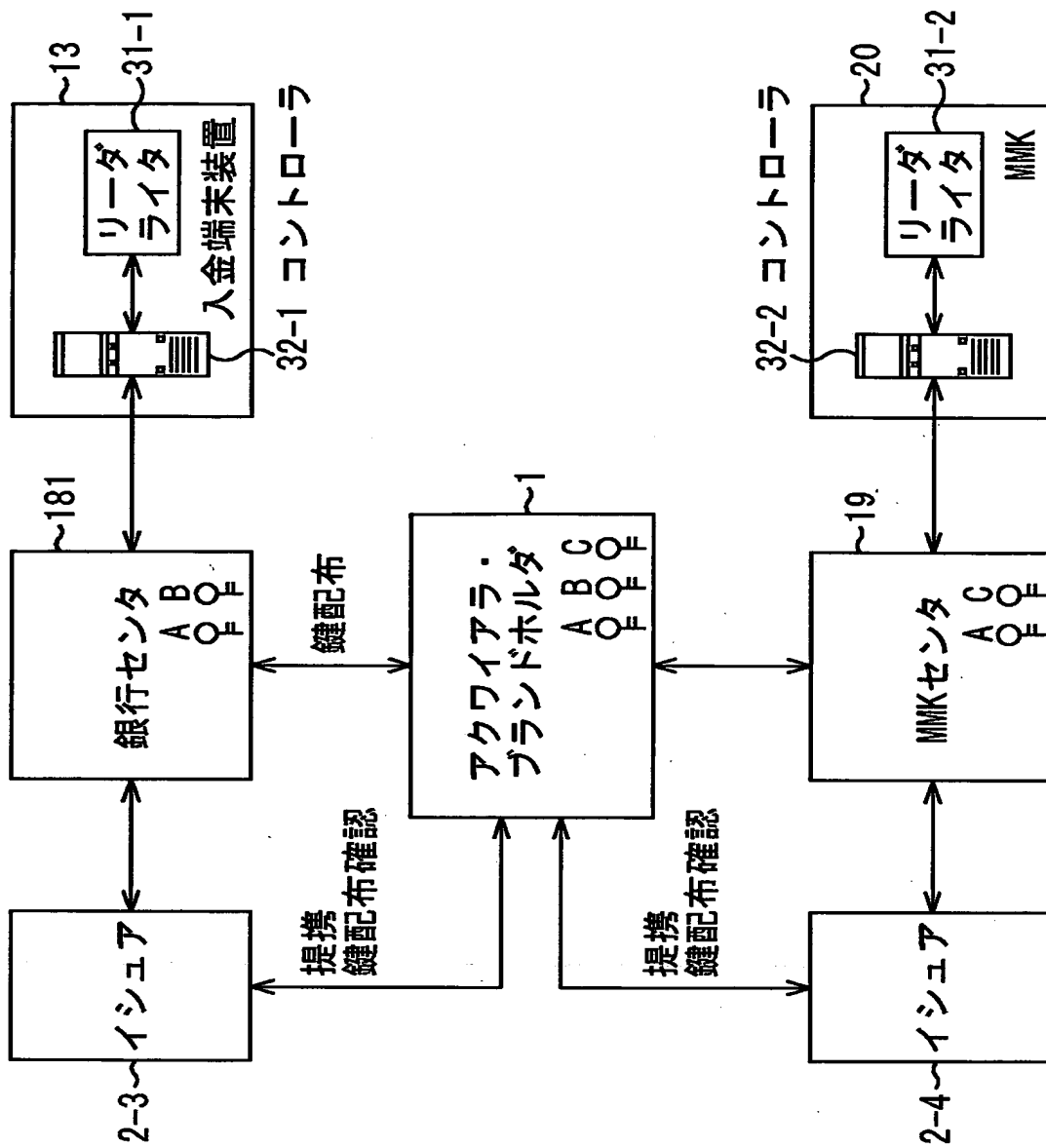


【図 11】

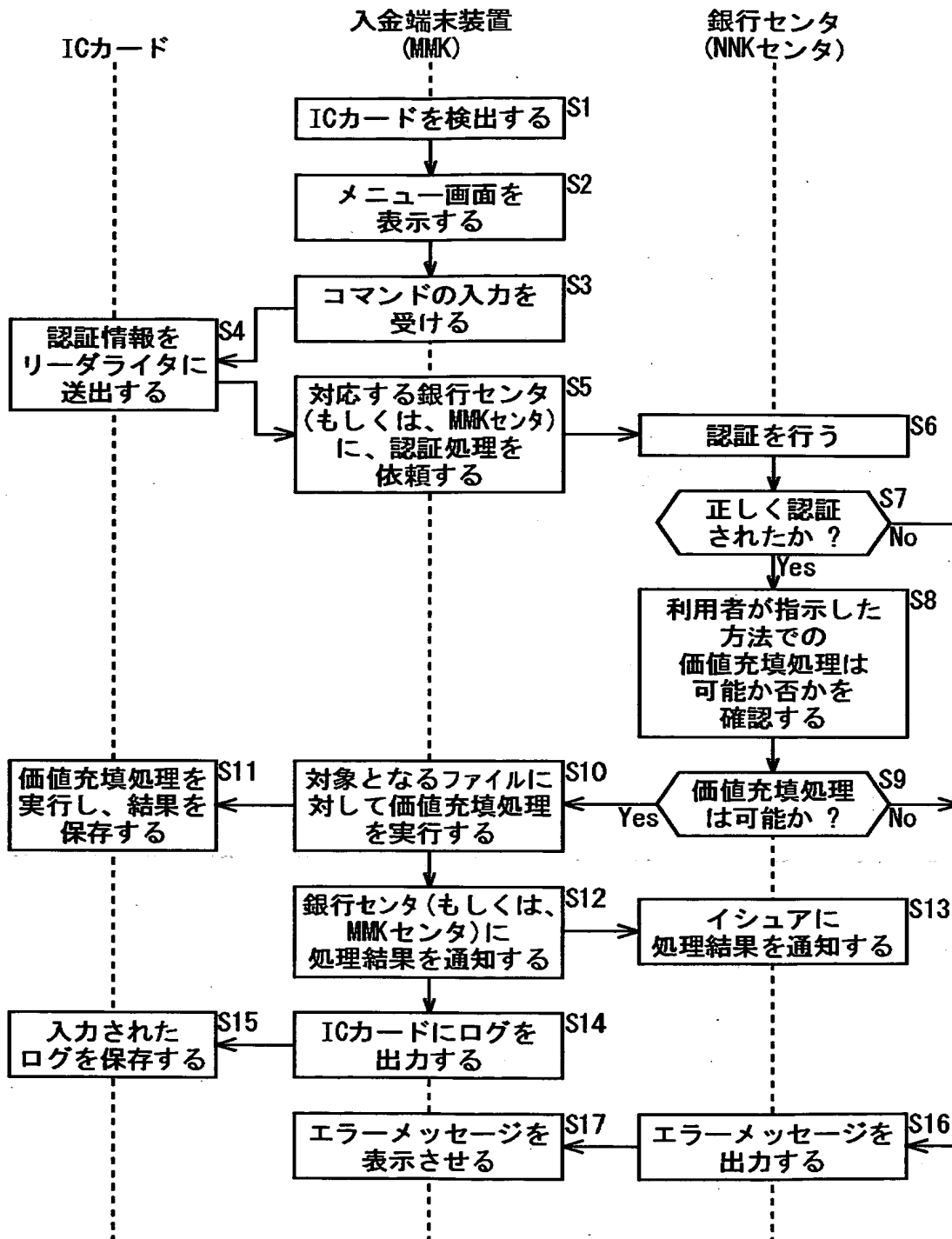


イシユア 2-2

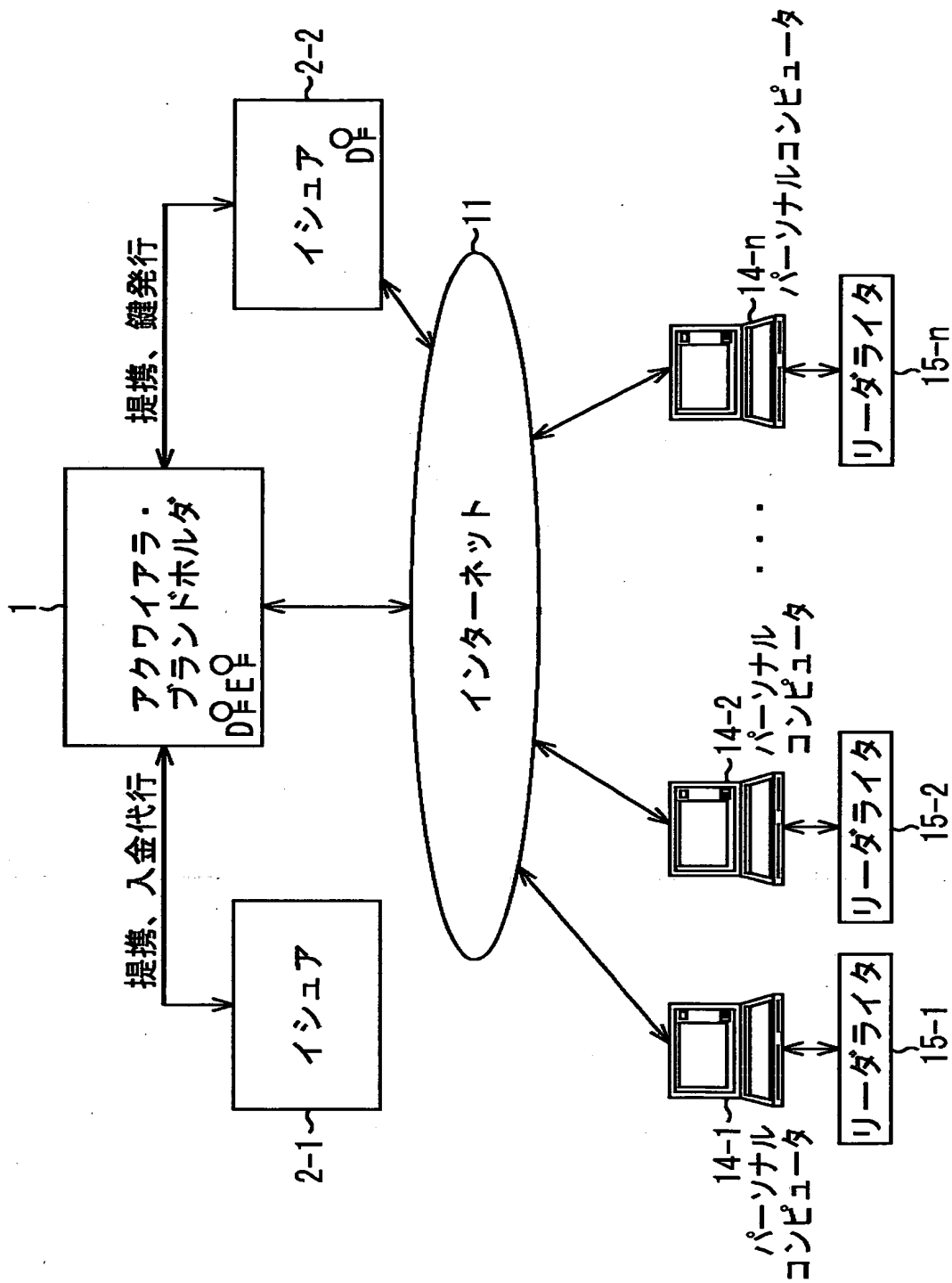
【図12】



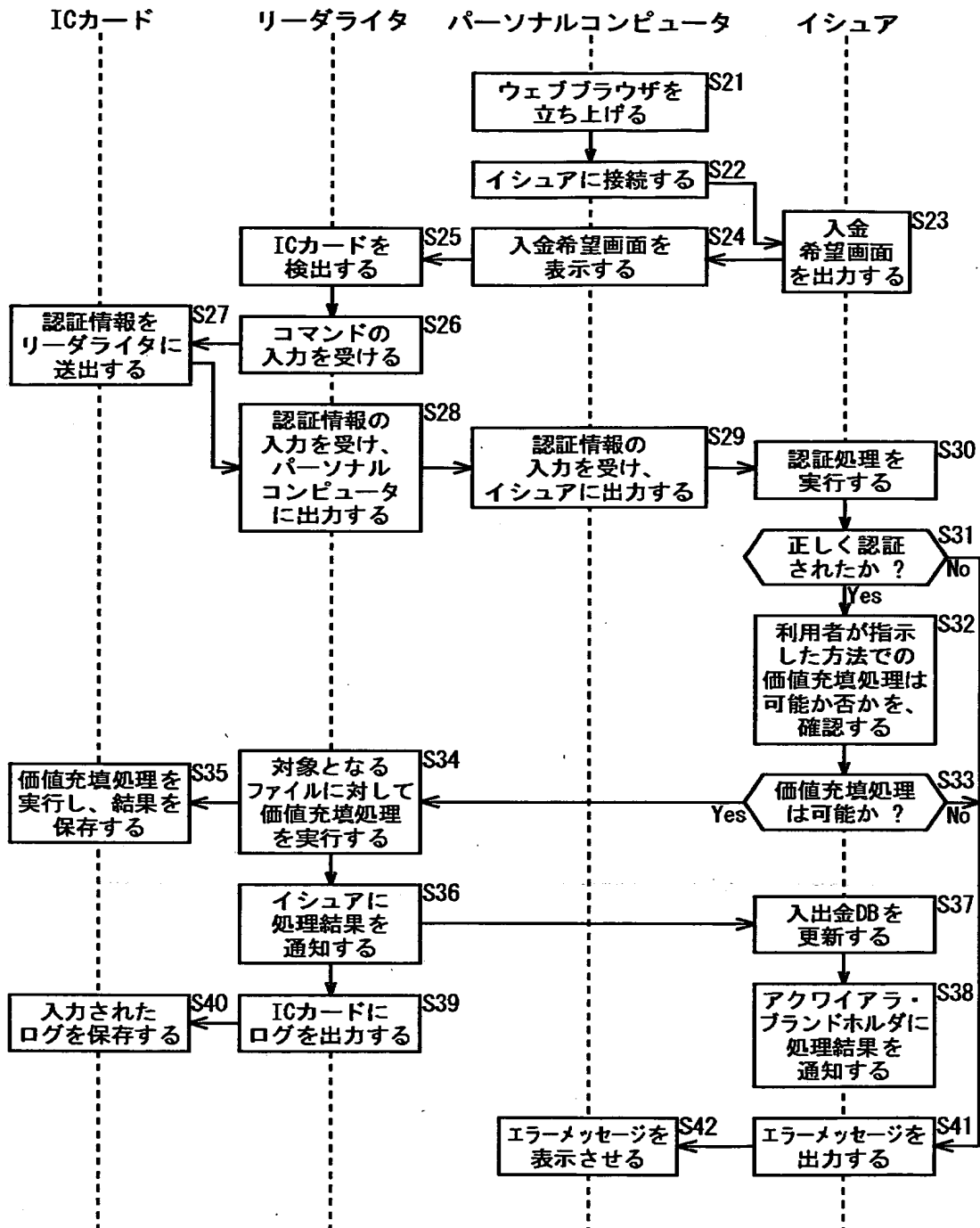
【図 1 3】



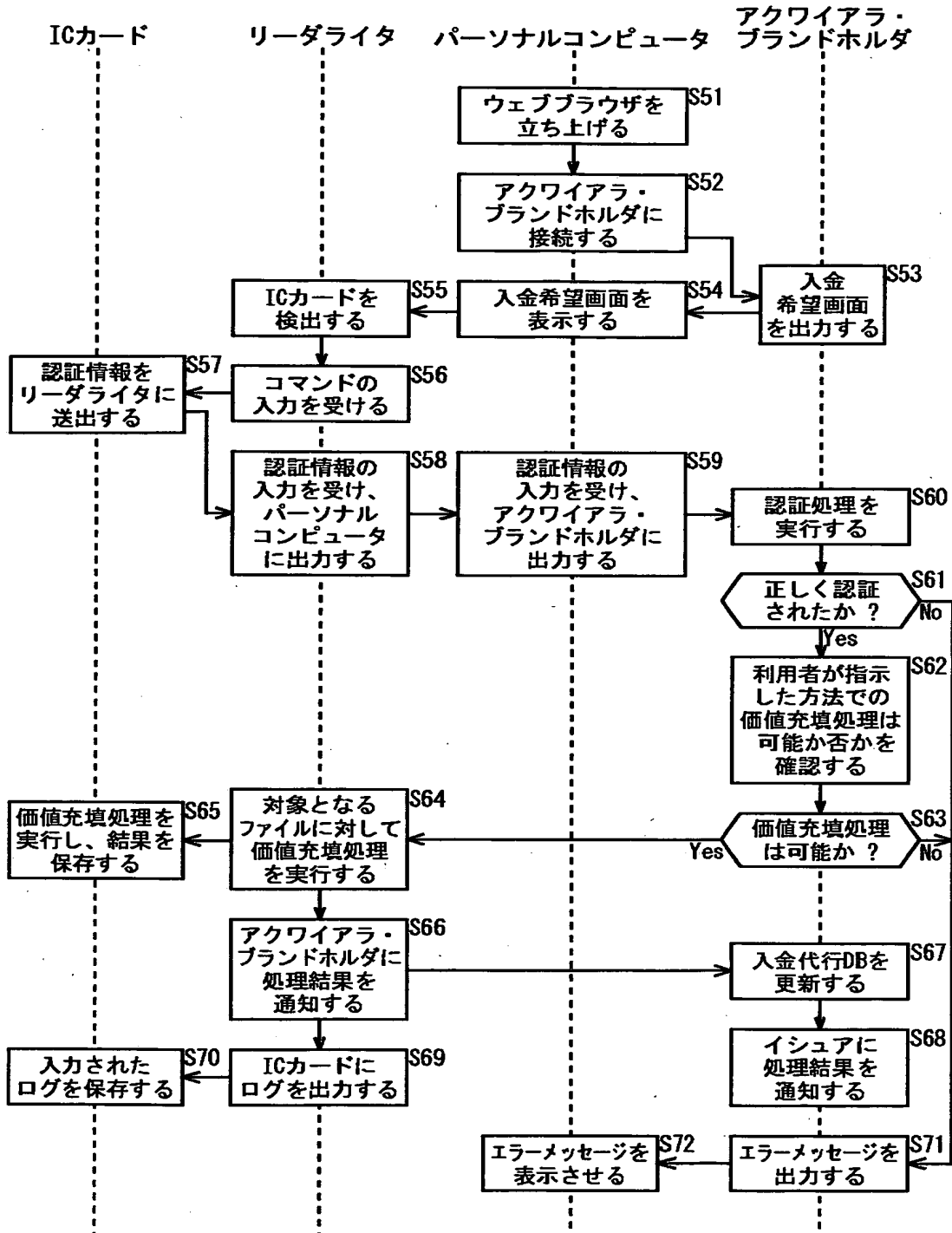
【図14】



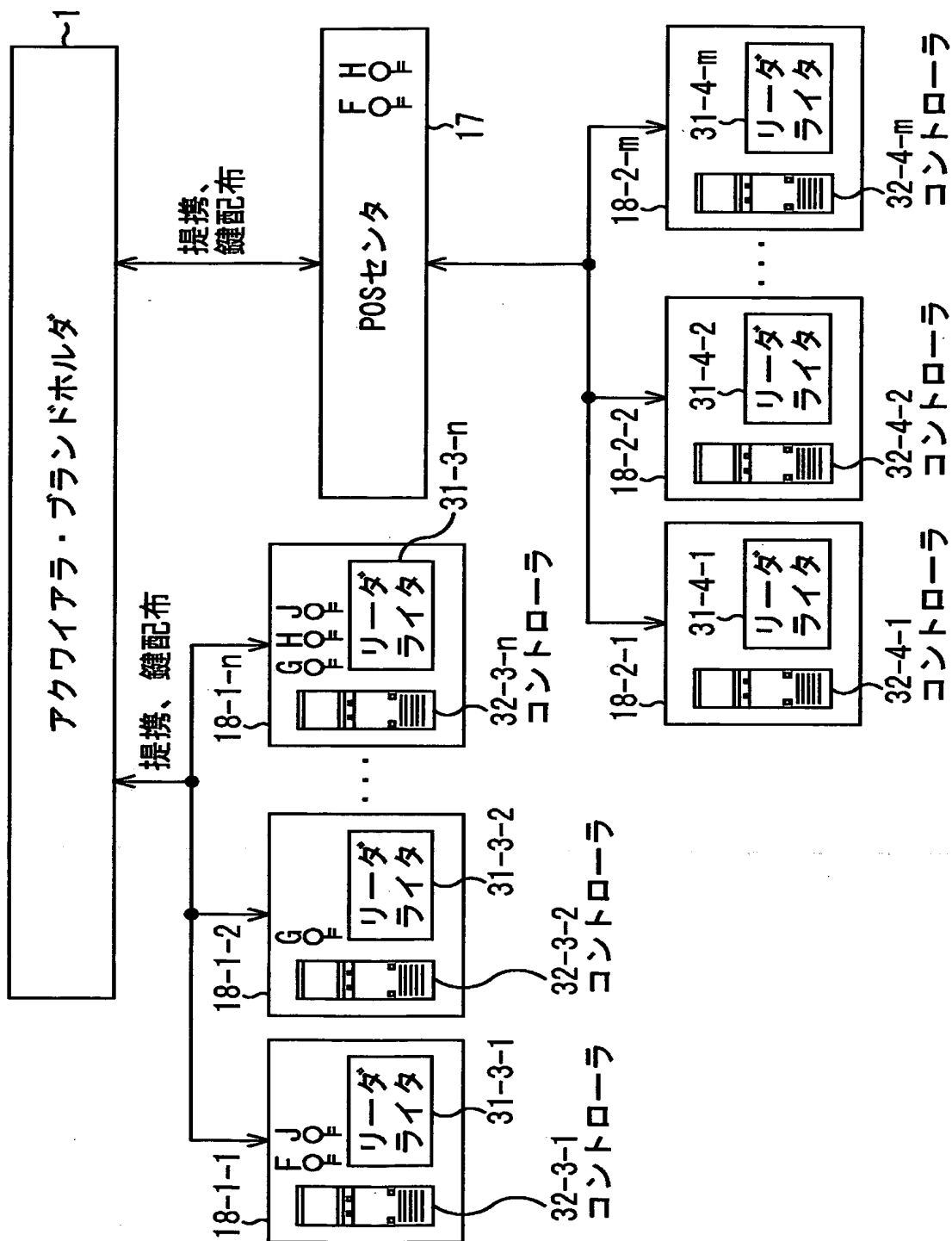
【図15】



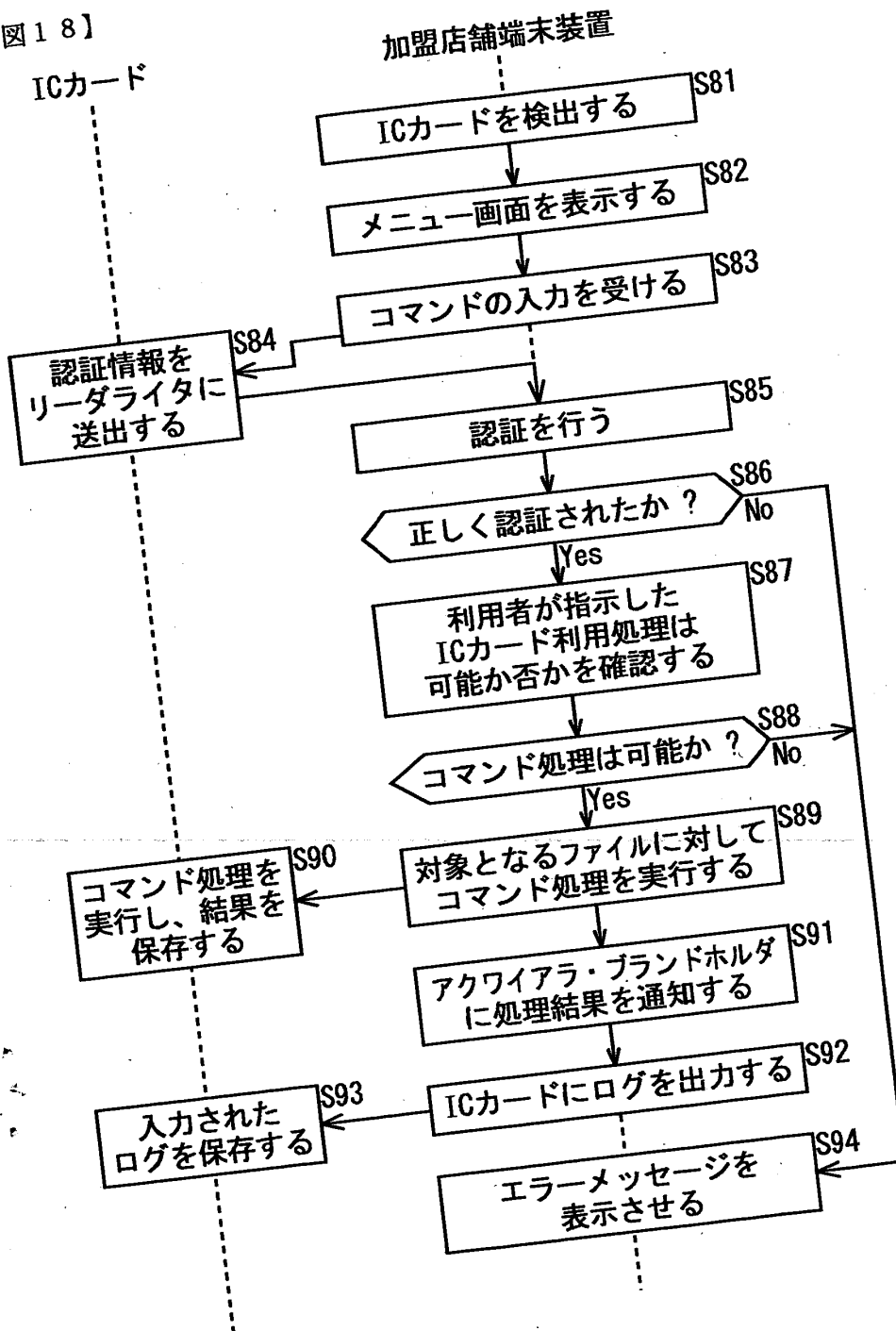
【図16】



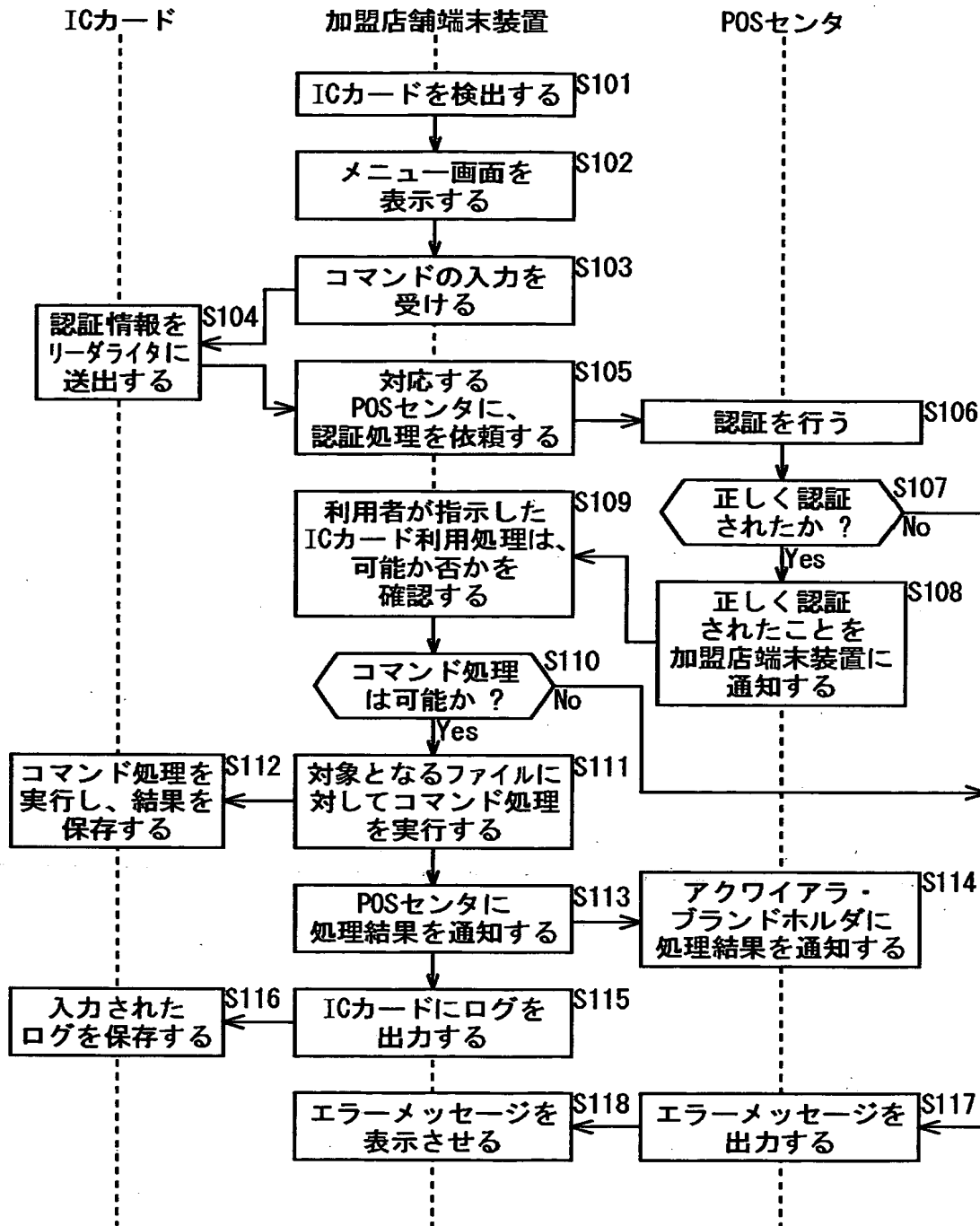
【図 17】



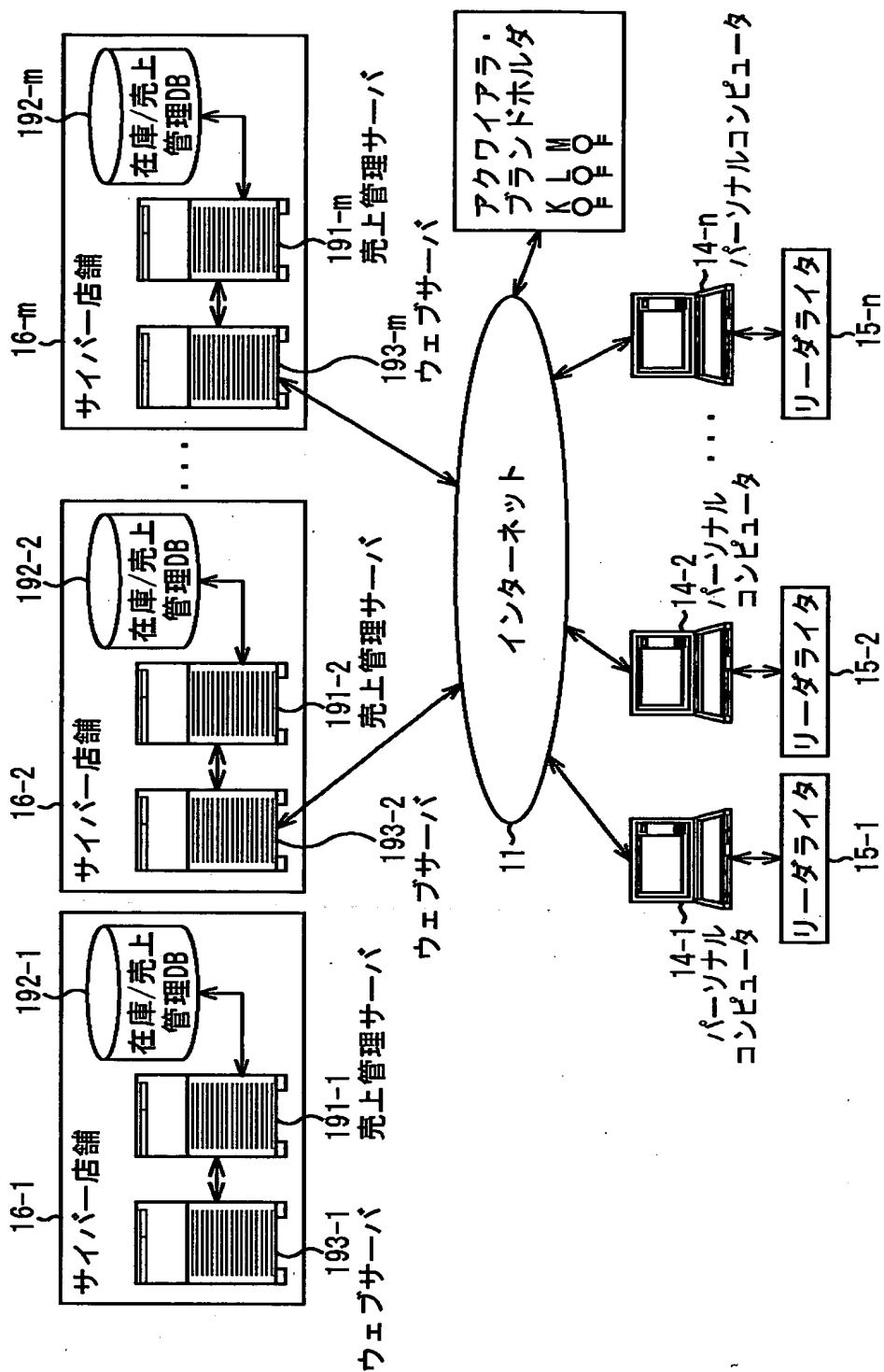
【図18】



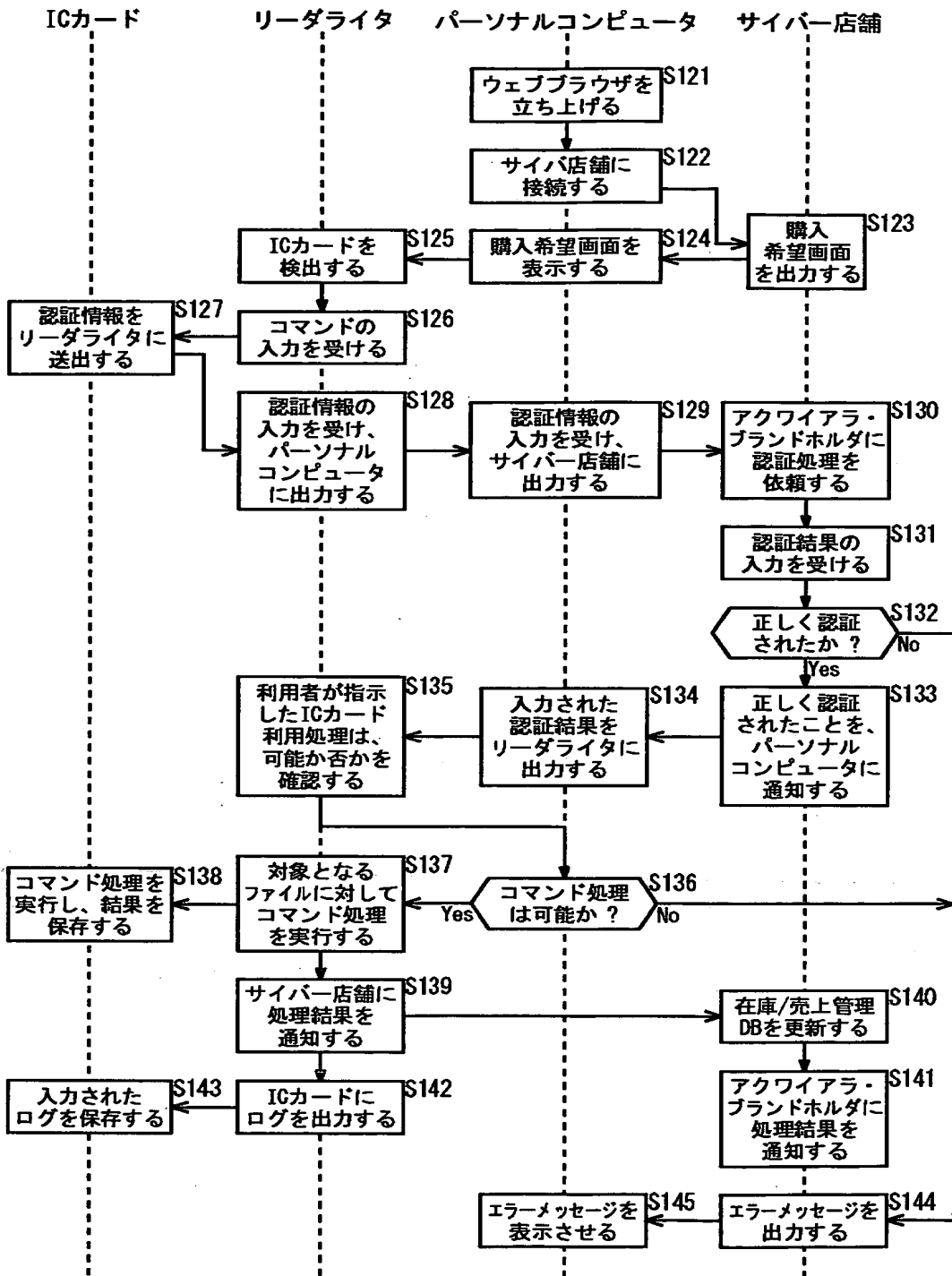
【図 19】



【図20】



【図 21】



【書類名】 要約書

【要約】

【課題】 管理・運営費が安価で、自由度の高い電子マネーシステムを構築する。

【解決手段】 電子マネーのブランドを管理するアクワイアラ・ブランドホルダ1は、本システムの認証処理に用いられる鍵を全て管理し、必要に応じて鍵を発行する。アクワイアラ・ブランドホルダ1は、ICカード12を発行するイシューア2、並びに、利用者がICカードを利用するための装置もしくはそれらを管理する装置である、POSセンタ17、MMKセンタ19、および加盟店端末装置21に対して、提携内容に基づいた鍵を配布するが、利用者が、パーソナルコンピュータ14およびリーダライタ15を用いて利用することができるサイバー店舗16には、発行した鍵を配布せずに、自分自身に保存し、サイバー店舗16からの要求に従って、所定のICカード12との認証処理を実行する。

【選択図】 図2

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日
[変更理由] 新規登録
住 所 東京都品川区北品川6丁目7番35号
氏 名 ソニー株式会社